

In the Matter of:

Communications Assistance for Law
Enforcement Act

REPLY COMMENTS REGARDING STANDARDS FOR ASSISTANCE CAPABILITY REQUIREMENTS

Louis J. Freeh, Director
Federal Bureau of Investigation

Larry R. Parkinson
General Counsel
Federal Bureau of Investigation
935 Pennsylvania Avenue, N.W.
Washington, D.C. 20535

Honorable Janet Reno
Attorney General of the United States

Stephen W. Preston
Deputy Assistant Attorney General

Douglas N. Letter
Appellate Litigation Counsel
Civil Division
U.S. Department of Justice
601 D Street, N.W., Room 9106
Washington, D.C. 20530
(202) 514-3602

TABLE OF CONTENTS

SUMMARY	1
DISCUSSION	3
I. The Commenters Misunderstand the Policies and Goals of CALEA and the Nature of this Proceeding	3
A. The Governing Policies and Goals of CALEA	3
B. The Present Proceeding	11
II. Each of the Capabilities Identified in the Government's Rulemaking Petition Is Included in the Assistance Capability Requirements of Section 103 of CALEA	15
A. Communications of Other Parties in Conference Calls	16
B. The Scope of "Call-Identifying Information"	30
C. Post-Cut-Through Dialing	38
D. Other Subject-Initiated Dialing and Signaling	45
E. Information on Participants in Multi-Party Calls	50
F. Notification of Network-Generated In-Band and Out-of-Band Signaling	55
G. Timely Delivery of Call-Identifying Information	59
H. Automated Delivery of Surveillance Status Information	66
I. Standardization of Delivery Interfaces	76
III. Other Assistance Capability Issues	78
A. Location Information	78
B. Packet Switching	80
C. Covered Carriers	80

SUMMARY

The Commission's request for public comments on the assistance capability requirements of the Communications Assistance for Law Enforcement Act (CALEA) has produced a voluminous body of comments. The Commission's burden in reviewing these comments and resolving the underlying disputes regarding the scope of CALEA's assistance capability requirements is a considerable one, and the Department of Justice and the FBI appreciate the effort and expertise that the Commission will bring to bear on the task. However, the legal force of the comments opposing the government's rulemaking petition in no way matches their physical weight. When the legal and technical arguments underlying the comments are carefully reviewed, the whole is much less than the sum of the parts.

At a general level, the comments reflect a fundamental misunderstanding of the policies and goals of CALEA. The preeminent concern of CALEA is, as the statute's very name suggests, the need for carriers to provide assistance to law enforcement in the execution of authorized electronic surveillance. The basic goal of CALEA's assistance capability requirements is to ensure that the technical ability of law enforcement to carry out electronic surveillance meets, rather than falls short of, law enforcement's legal authority. The commenters who suggest that law enforcement concerns are of no more than secondary importance for CALEA, or that CALEA should be read in ways that limit the ability of law enforcement to carry out legally authorized surveillance, are disregarding the basic underpinnings of the statutory scheme.

At a more specific level, the comments fail to come to terms with the showing in the government's rulemaking petition regarding the deficiencies in the interim standard. Contrary to the commenters' claims, each of the capabilities missing from the interim standard and requested in the

government's petition is firmly rooted in the language, legislative history, and policies of CALEA, and the failure to provide these capabilities will result in serious injury to the government's ability to enforce state and federal laws through electronic surveillance. The commenters' objections to the individual capabilities at issue in this proceeding reflect both legal errors regarding CALEA and the underlying electronic surveillance statutes and technical errors regarding network capabilities and the operation of the interim standard itself. We discuss these errors in detail in this filing. Once they are understood, it will be clear that the government's petition lies at the heart of CALEA, not (as the commenters suggest) beyond CALEA's outer limits.

The Commission is now being called on to perform a task that is critical to the proper implementation of CALEA. Section 103 of CALEA imposes mandatory assistance capability obligations that must be met by all telecommunications carriers. At the same time, CALEA's "safe harbor" provision means that, absent action by the Commission, industry-promulgated standards effectively replace the underlying statutory requirements of Section 103. Unless the interim standard is adequate to ensure that every carrier that implements it is thereby satisfying its underlying statutory requirements of Section 103 in all of the respects at issue in this proceeding, the interim standard works a pro tanto repeal of Section 103 itself. Congress vested the Commission with authority to act under Section 107(b) of CALEA precisely in order to avoid that result. Only prompt action and rigorous review by the Commission can ensure that the assistance capability requirements of Section 103, and the manifest public interests in law enforcement and personal safety that underlie those requirements, are fully vindicated.

DISCUSSION

The Department of Justice and the FBI submit these reply comments in response to comments filed by other parties on May 20, 1998, regarding the assistance capability requirements of Section 103 of CALEA. The following discussion is divided into three parts. In Part I, we respond to comments concerning the general purpose and scope of CALEA and the nature of the present rulemaking proceeding. In Part II, we respond to comments directed at the specific assistance capabilities addressed in the government's petition and proposed rule. In Part III, we address comments dealing with other assistance capability issues.

I. The Commenters Misunderstand the Policies and Goals of CALEA and the Nature of this Proceeding

A. The Governing Policies and Goals of CALEA

1. This proceeding involves the Communications Assistance for Law Enforcement Act. We begin by underscoring the title of the Act because it reflects a basic truth that many of the commenters prefer to ignore: the obligation of the telecommunications industry to assist law enforcement constitutes the heart of CALEA.

The enactment of CALEA was not sought by the telecommunications industry, nor was it sought by privacy groups. Instead, Congress acted in response to the unanimous requests of federal, state, and local law enforcement agencies for assistance in the execution of lawful electronic surveillance. Congress acted to "insure that law enforcement can continue to conduct authorized wiretaps" in the face of rapid technological changes in the telecommunications industry. H. Rep. No. 103-827, 103d Cong., 2d Sess. 9 (1994) ("House Report"), reprinted in 1994 U.S. Code Cong. & Admin. News ("USCCAN") 3489; Digital Telephony and Law Enforcement Access to Advanced

Telecommunications Technologies and Services: Joint Hearings before the Subcomm. on Technology and the Law, Senate Comm. on the Judiciary, and Subcomm. on Civil and Constitutional Rights, House Comm. on the Judiciary ("Joint Hearings"), 103d Cong., 2d Sess. 109 (Aug. 11, 1994) (statement of Sen. Leahy) (CALEA "will assure law enforcement's ability to conduct court-authorized wiretaps").

To be sure, assisting law enforcement in the performance of authorized electronic surveillance is not the only goal of CALEA. Congress also sought to accommodate other interests, such as the continued development of new communications technologies and the protection of specified privacy interests, and Section 107(b) of CALEA requires the Commission to take account of those interests in framing technical requirements and standards in this proceeding. But while assisting law enforcement is not the only goal of CALEA, it is manifestly the preeminent one. Section 103(a) imposes specific assistance capability obligations on telecommunications carriers that must be met by all equipment, facilities, and services installed or deployed after January 1, 1995. And Section 107(b) mandates that any technical requirements and standards issued by the Commission in this proceeding must "meet the assistance capability requirements of section 103 * * * ." 47 U.S.C. § 1006(b)(1). Law enforcement's need for assistance in the performance of authorized electronic surveillance is thus fundamental to the scope and operation of CALEA, and it must play an equally central role in the Commission's implementation of the statute.

The comments submitted by privacy groups, such as the Center for Democracy and Technology ("CDT") and the Electronic Privacy Information Center ("EPIC"), are particularly notable for their failure to come to terms with this principle. CDT and EPIC make the remarkable assertion that the principal goal of CALEA is to protect privacy, and that law enforcement concerns

are merely secondary. See, e.g., CDT Comments at 15 ("Congress * * * has placed privacy interests in front of law enforcement"); EPIC Comments at 4 ("privacy interests [must be] accorded the highest priority in the implementation of CALEA"). This assertion simply cannot be sustained.

CALEA does contain a number of discrete provisions that were framed in response to privacy concerns, but most of those provisions are simply irrelevant to this proceeding. See, e.g., CALEA § 202 (codified at 18 U.S.C. §§ 2510(1), 2510(12), 2511(4)(b)) (cordless telephones); id. § 203 (codified at 18 U.S.C. § 2510(16)) (radio-based data communications); id. § 204 (codified at 18 U.S.C. § 2511(4)(b)) (spread spectrum radio communications). In contrast, the assistance capability requirements of Section 103, which form the basis for this proceeding, are framed primarily in terms of satisfying law enforcement's need for assistance in the execution of lawful electronic surveillance. Three of the four assistance capability requirements in Section 103 (47 U.S.C. § 1002(a)(1)-(3)) are directed specifically toward facilitating electronic surveillance, and the fourth (47 U.S.C. § 1002(a)(4)) addresses law enforcement needs as well as privacy concerns. The notion that Section 103 is designed principally to further privacy interests simply cannot be reconciled with the terms of the statute.

2. In an effort to limit the scope of the Commission's review of the interim standard, a number of the commenters point to statements in the House Report that urge against "an overbroad interpretation of the [Section 103] requirements" and encourage "industry, law enforcement, and the FCC to narrowly interpret the requirements." House Report at 23, reprinted in 1994 USCCAN at 3503. We have no quarrel with the general proposition that overbroad interpretations of Section 103 should be avoided. But that general proposition is of little assistance in resolving disputes over the specific capabilities at issue in this proceeding.

In particular, it will not do to argue, as various commenters do regarding particular assistance capability issues, that the government's position must be incorrect because it is "broad" or because industry's contrary position is "narrow." Simply labeling a position in conclusory fashion as "broad" or "narrow" does not advance the legal analysis. Something more is required: careful attention to the language and legislative policies of CALEA as they apply to the particular assistance capability in question. In the government's view, when the interim standard is reviewed in this manner, it is demonstrably deficient as a means of ensuring that the assistance capability requirements of Section 103 are met, even when those requirements are construed narrowly.

In a related vein, several commenters argue that the government is trying to undo legislative compromises that Congress incorporated in CALEA. See, e.g., TIA Comments at i, v. The commenters are correct that CALEA reflects legislative compromises. See, e.g., Joint Hearings at 112-14 (statement of FBI Director Freeh). But they are fundamentally mistaken that the government is seeking to undo those compromises.

The compromises reached during the development of CALEA are embodied in the terms of CALEA itself. The government seeks nothing more than the implementation of technical requirements and standards that fully comport with those terms. For reasons set forth in the government's petition, and addressed in further detail in this filing, the government believes that the interim standard falls well short of ensuring that the explicit assistance capability requirements of Section 103 will be met by carriers who adhere to that standard. Congress vested this Commission with authority to act under Section 107(b) precisely because it foresaw that the telecommunications industry might, for a variety of reasons, develop technical standards that do not adequately implement

the statutory mandates of Section 103. In asking the Commission to adopt additional technical requirements and standards, we are seeking to preserve, not upset, the balance struck by Congress.

Moreover, it is important to recognize that the compromises embodied in CALEA run in both directions; while law enforcement yielded ground in some areas during the legislative process, it gained in others. For example, Congress replaced "call setup information" in the original draft legislation with "call-identifying information" in CALEA, and as explained in detail below (see pp. 31-32 infra), the final definition of "call-identifying information" (47 U.S.C. § 1001(2)) is more inclusive than the original definition of "call setup information." It is thus a fundamental distortion of the legislative record for commenters to suggest that Congress acted only to pare back law enforcement's original proposals during the drafting of CALEA, and that the government is now trying to reverse that process in this proceeding.

3. Several commenters argue that the legislative history demonstrates that CALEA is intended to provide law enforcement with the same capability to conduct electronic surveillance that law enforcement traditionally had in the analog POTS environment, and no more. See, e.g., EPIC Comments at 16-18; Americans for Tax Reform ("ATR") Comments at 8, 15, 21. Based on that premise, the commenters argue that the government's petition is facially invalid to the extent that it seeks access to information that the government could not traditionally acquire by monitoring the "local loop" between a subscriber and the subscriber's central office. See, e.g., BellSouth Comments at 8. These comments confuse two fundamentally different issues: the technical capability to engage in electronic surveillance and the legal authority to do so. The failure to distinguish between technical capability and legal authority is one of the most fundamental and pervasive errors made by the commenters in this proceeding.

As noted in the government's petition, the legal authority of federal, state, and local law enforcement agencies to engage in electronic surveillance is governed principally by Title III of the Omnibus Crime Control and Safe Streets Act of 1968 ("Title III") and the Electronic Communications Privacy Act of 1986 ("ECPA"). See DOJ/FBI Petition at 6-7; see also Notice of Proposed Rulemaking, In the Matter of Communications Assistance for Law Enforcement Act, CC Docket No. 97-213 (released Oct. 10, 1997), at 4-8. These statutes establish substantive and procedural rules for the interception of wire and electronic communications and the acquisition of related dialing and signaling information. See generally 18 U.S.C. §§ 2510-21, 3121-27.

Section 103 of CALEA, in contrast, is directed at the technical capability of law enforcement to carry out electronic surveillance. It prescribes the obligations of telecommunications carriers to assist law enforcement in acquiring communications and call-identifying information "pursuant to a court order or other lawful authorization." 47 U.S.C. § 1002(a)(1)-(3). Section 103 does not purport to define or alter the scope of the legal authority conferred by Title III and ECPA. It presupposes the existence of legal authorization and directs carriers to provide specified assistance so that law enforcement has the capability to carry out the authorized surveillance.

In arguing that the legislative history of CALEA shows an intention to freeze the traditional surveillance capabilities of law enforcement, the commenters point chiefly to the testimony of FBI Director Freeh. Director Freeh's cited testimony, however, was explicitly directed at the issue of legal authority, not that of surveillance capabilities. Director Freeh testified that "[w]e are not seeking any expansion of the authority Congress gave to law enforcement when the wiretapping law was enacted 25 years ago"; that "[t]he proposed legislation * * * does not alter the Government's authority to conduct court-authorized electronic surveillance and use pen registers or trap and trace devices"; and

that "[w]e are not asking * * * to expand the authority that we have to do wiretapping." Joint Hearings at 6, 7, 10 (emphasis added). It is this testimony to which the House Report on CALEA is referring when it states that "[t]he FBI Director testified that the legislation was intended to preserve the status quo * * * ." House Report at 22, reprinted in 1994 USCCAN at 3502; compare Joint Hearings at 32 (prepared statement of Director Freeh) (proposed legislation "ensures a status quo as it relates to legal authorities" governing electronic surveillance)) (emphasis added).

While Director Freeh's testimony makes clear that CALEA was not intended to alter the general legal authority of law enforcement to conduct electronic surveillance, nothing in his testimony -- or anywhere else in the legislative history -- suggests that Congress meant to freeze or otherwise limit law enforcement's technical capability to perform authorized electronic surveillance. To the contrary, Director Freeh testified that the proposed legislation was intended "to maintain technological capabilities commensurate with existing legal authority" -- to ensure, in other words, that law enforcement's technical capability to perform electronic surveillance would not fall short of its legal authorization to do so. Joint Hearings at 7 (emphasis added); see also id. at 6 ("We simply seek to ensure a failsafe way for law enforcement to conduct court-authorized wiretapping on the recently deployed and emerging technology."). The House Report sounds the same note when it states that CALEA is intended "[t]o insure that law enforcement can continue to conduct authorized wiretaps in the future * * * ." House Report at 9, reprinted in 1994 USCCAN at 3489; see also 140 Cong. Rec. S11055 (Aug. 9, 1994) (Sen. Leahy) (CALEA "will give our law enforcement agencies back the confidence that when they get a wiretap order, they will be able to do their jobs and carry out the order"). The House Report makes clear that CALEA was intended not only to prevent the erosion of existing surveillance capabilities through the introduction of new technologies, but also to

deal with "impediments to authorized wiretaps, like call forwarding, [that] have long existed in the analog environment." Id. at 12, reprinted in 1994 USCCAN at 3492.

The focus of the present rulemaking proceeding is the assistance capability requirements of Section 103 of CALEA, not the underlying legal authorization conferred by Title III and ECPA. The provisions of the government's proposed rule do not purport to alter the boundaries of the government's legal authority to engage in electronic surveillance. Regardless of whether a carrier has the technical capability to provide particular information to law enforcement, law enforcement may not obtain that information unless it has a court order or other sufficient legal authorization. That is true of the TIA interim standard; it is equally true of the standards in the government's proposed rule. As a result, a decision by the Commission to issue the proposed rule, or to modify the terms of the interim standard in some other fashion, will not expand the legal authority of law enforcement to conduct electronic surveillance in any way. To the extent that the commenters suggest otherwise, they are simply and indisputably mistaken.

4. As the foregoing discussion of surveillance capabilities indicates, whether law enforcement traditionally has had the capability to obtain a particular kind of call content or call-identifying information is not dispositive for purposes of this proceeding. The assistance capability obligations of telecommunications carriers under CALEA are specifically defined by Section 103(a). If a particular capability does not come within the scope of Section 103(a), carriers are not legally obligated by CALEA to maintain that capability, regardless of historical practice.¹ But if a particular

¹ It should be borne in mind, however, that CALEA is only one source of a carrier's legal obligations to assist law enforcement. A carrier has independent assistance obligations that are not superseded or relieved by CALEA. House Report at 20, reprinted in 1994 USCCAN at 3500 ("The assistance capability and capacity requirements of the bill are in addition to the existing necessary (continued...)")

capability does come within the scope of Section 103(a), then CALEA obligates carriers to provide it, even if law enforcement did not historically have the technical ability to acquire such information. See DOJ/FBI Petition ¶ 45.

At the same time, law enforcement's traditional capabilities are hardly irrelevant, as some commenters suggest. The principal (although not exclusive) impetus for the enactment of CALEA was the impact of technological changes on the execution of authorized electronic surveillance. See, e.g., House Report at 11-16, reprinted in 1994 USCCAN at 3491-96. Whatever disputes may exist about the purposes underlying CALEA, it cannot seriously be disputed that Congress sought to "ensure that new technologies and services do not hinder [authorized] law enforcement access" to electronic communications. Id. at 16, reprinted in 1994 USCCAN at 3496. The interim standard, however, falls well short of realizing that goal. To the extent that the interim standard deprives law enforcement of the ability to obtain call content and call-identifying information to which it historically has had access, industry should bear a substantial burden to show that the interim standard is not deficient.

B. The Present Proceeding

1. The government's rulemaking petition grows out of the "safe harbor" provisions of Section 107 of CALEA. When an industry association or standard-setting organization issues technical requirements or standards intended "to meet the [assistance capability] requirements of section 103," the industry standards constitute a safe harbor for telecommunications carriers. 47

¹(...continued)
assistance requirements" in Title 18 and Title 50); see, e.g., 18 U.S.C. 2518(4) (duty to furnish "all information, facilities, and technical assistance necessary to accomplish the interception unobtrusively and with a minimum of interference with the [subject's] services"); United States v. New York Telephone Co., 434 U.S. 159, 177 (1977).

U.S.C. 1006(a)(2).² If the Commission promulgates standards under Section 107(b), the Commission's standards likewise constitute a safe harbor, one that supersedes any industry standards to the extent that they differ. Ibid. The ultimate question presented to the Commission by the government's rulemaking petition and the other petitions is whether, and how, the Commission should alter the boundaries of the safe harbor created by the industry's interim standard.

For purposes of this proceeding, it is critical for the Commission to bear in mind two points regarding the operation of CALEA's safe harbor provision. The first is that, by virtue of the provision, an industry standard effectively redefines the statutory assistance capability requirements of Section 103 for any carrier that chooses to observe the standard (until and unless the industry standard is revised by the Commission). Under Section 107(a)(2) of CALEA, a carrier that complies with an industry standard "shall be found to be in compliance with the assistance capability requirements under section 103 * * *." 47 U.S.C. 1006(a)(2). Thus, a carrier that meets the industry standard has no other legal obligations under Section 103, unless and until the industry standard is changed by the Commission.³

If an industry standard is sufficiently rigorous to ensure that carriers who satisfy it are in fact meeting the assistance capability requirements of Section 103 in all respects, then the integrity of the statutory scheme is preserved. But if (or to the extent that) an industry standard does not ensure

² In order to provide a safe harbor, industry standards must be "designed in good faith to implement the assistance requirements." House Report at 26, reprinted in 1994 USCCAN at 3506 (emphasis added). If industry standards were a sham or otherwise did not represent a good faith attempt to meet the requirements of Section 103, they would not constitute a safe harbor.

³ We assume for purposes of this discussion that an industry standard has not been rendered obsolete or incomplete by subsequent technological developments. The issue of whether an industry standard would continue to provide a safe harbor if industry refused to update the standard in response to such developments is not presented here and need not be addressed by the Commission.

that carriers will meet the requirements of Section 103, it amounts to a pro tanto repeal of those requirements; it works to excuse carriers from meeting specific legal obligations imposed on them by Congress.

It is therefore imperative for the Commission to scrutinize the adequacy of the interim standard with the greatest possible care. Unless the Commission is satisfied that the interim standard is sufficiently comprehensive to ensure that all carriers covered by the interim standard are meeting their obligations under Section 103 with respect to every capability at issue in this proceeding, the interim standard is deficient and the Commission must act to prevent an impermissible diminution of the statutory requirements of Section 103. By the same token, any standards adopted by the Commission must likewise be sufficient to ensure that all carriers who meet the standard are in fact satisfying all of their underlying statutory obligations under Section 103.

The second point to bear in mind is that no carrier is legally obligated to employ the particular means of satisfying Section 103 that are set forth in the safe-harbor standard, regardless of whether the standard is set by industry or by the Commission. As explained in the government's May 20 comments, the safe harbor mechanism created by Section 107(a)(2) is a voluntary one. If a carrier can satisfy its underlying assistance capability obligations under Section 103 by other means, it is free to do so; failure to use the specific means set forth in the safe-harbor standard does not itself render the carrier's conduct unlawful.⁴

⁴ As explained in the government's May 20 comments, this does not mean that carriers are free to disregard the Commission's conclusions regarding the underlying assistance capability requirements of Section 103 themselves. To the extent that the Commission's standards identify statutorily required capabilities, carriers must meet those capabilities. See DOJ/FBI Comments ¶¶ 27-28. The particular means of meeting the capabilities, however, are not confined to those specified in the Commission's standards.

The voluntary character of the safe-harbor standard bears directly on the nature of the Commission's task in this proceeding. Because the specific means prescribed by the safe-harbor standard are voluntary, the Commission need not pursue a "lowest common denominator" approach that attempts to accommodate the potentially differing circumstances of each individual carrier and each platform. If the standards developed by the Commission in this proceeding pose practical problems for carriers using particular equipment or network configurations, those carriers are under no obligation to use the means set forth in the Commission's standards. If they can satisfy their underlying obligations under Section 103 by other means that are better suited to their particular circumstances, they are free to do so. And if compliance with Section 103 is not "reasonably achievable" with respect to particular equipment, facilities, or services, whether for reasons of cost or for other reasons, a carrier is free to seek relief from the Commission under Section 109(b) of CALEA (47 U.S.C. § 1008(b)). The Commission therefore can develop standards that "meet the assistance capability requirements of section 103" (47 U.S.C. § 1006(b)(1)) without having to tailor those standards to the peculiar circumstances of individual carriers and platforms.

2. At this stage of this proceeding, the Commission's principal focus should be on the adequacy of the interim standard, not the particulars of the government's proposed rule. At various points, commenters take issue with one or another detail of the provisions in the proposed rule -- for example, the desirability of a 100-millisecond time stamp in comparison with alternative arrangements. We address many of these comments in the course of the following discussion. But arguments directed at the details of the proposed rule are distinct from, and no substitute for, arguments defending the adequacy of the interim standard itself. If the interim standard is deficient,

the Commission is obligated to issue new standards that correct the deficiencies.⁵ Arguments about how the deficiencies should be corrected, and whether the government's proposed rule represents the most desirable means of doing so, are best left for the round of comments that will follow the issuance of an NPRM.

II. Each of the Capabilities Identified in the Government's Rulemaking Petition Is Included in the Assistance Capability Requirements of Section 103 of CALEA

The government's rulemaking petition identifies a number of specific capabilities that have been omitted from the interim standard but that are, in the government's view, required in order to ensure that carriers will actually satisfy their assistance capability obligations under Section 103 of CALEA. See generally DOJ/FBI Petition ¶¶ 42-105. We now respond to the comments regarding each of these capabilities in turn. At the outset, however, one preliminary point is in order: every one of the capabilities in the government's petition was originally included by industry itself in the initial working draft documents for the industry standard.

Industry circulated its initial draft standards document (PN 3580) in October 1995. The initial drafts included all of the capabilities that are now in dispute. Having originally included each of these capabilities, industry subsequently revised the draft standard during the course of the following year to exclude them, pruning hundreds of pages from the standard in the process.

⁵ US West argues that the Commission need not (and should not) issue corrective standards even if it determines that the interim standard is deficient. See US West Comments at i, 25-27. This argument is entirely incorrect. Section 301 of CALEA provides that "[t]he Commission shall prescribe such rules as are necessary to implement the requirements of" CALEA. 47 U.S.C. § 229(a) (emphasis added). If the interim standard does not meet the assistance capability requirements of Section 103, the Commission therefore must prescribe, by rule, standards that meet those requirements. The factors set forth in Section 107(b), such as cost-effectiveness and impact on residential ratepayers, concern how the assistance capability requirements of Section 103 are to be met, not (as US West suggests) whether they are to be met at all.

The fact that industry itself originally included these capabilities in its own draft standard makes the tone of disbelief that pervades many industry comments something less than convincing. Although industry repeatedly suggests that there is no legal basis in CALEA for the capabilities requested by the government, industry itself evidently shared law enforcement's interpretation of CALEA at the outset of the standard-setting process. In addition, the fact that industry originally agreed with these capabilities, only to retreat from them later, casts a rather different light on the standard-setting process from the one reflected in the industry comments here. These comments paint a picture of a process in which industry made every reasonable attempt (and then some) to accommodate law enforcement, while law enforcement responded by advancing ever-increasing demands. With respect to the "punch list" items, these comments get the matter exactly backward: far from making concessions, industry retreated dramatically from its own original position, and law enforcement's efforts were directed at bringing industry back to the point where it started. That effort was unsuccessful; this proceeding is the necessary result.

A. Communications of Other Parties in Conference Calls

The first capability at issue is the ability to intercept the communications of all parties in a conference call supported by the subscriber's equipment, facilities, or services. The interim standard only permits law enforcement to intercept those communications that are occurring over the leg of the call to which the subscriber's terminal equipment is actually connected (and hence audible to the intercept subject) at any point in time. See J-STD-025 § 4.5.1; TIA Comments at 31 & n.74. As a result, if other parties to the conference call talk to each other when the subject places them on hold or drops off the call, the interim standard does not provide access to those communications. Communications between other parties to a conference call may have substantial investigatory and

evidentiary value to law enforcement, regardless of whether the subject (who may not even be the person suspected of criminal activity) is "on the line." For reasons outlined in the government's petition, these communications come squarely within the scope of Section 103(a)(1) of CALEA, which obligates carriers to provide law enforcement with "all wire and electronic communications carried by the carrier within a service area to or from equipment, facilities, or services of a subscriber * * * ." 47 U.S.C. § 1002(a)(1); see also House Report at 9, reprinted in 1994 USCCAN at 3489 (CALEA intended to assist law enforcement in intercepting communications "involving * * * features and services such as call forwarding, speed dialing and conference calling") (emphasis added). The omission of these communications therefore renders the interim standard seriously deficient. See DOJ/FBI Petition ¶¶ 46-56.

TIA and other commenters argue that the communications of other parties to a conference call are outside the scope of Section 103(a)(1) when the subject is "off the call." See, e.g., TIA Comments at 31-33; CDT Comments at 39-40. They also argue that Title III does not authorize law enforcement to intercept such communications. See, e.g., TIA Comments at 34-38; Ameritech Comments at 3-5. As we now show, both arguments are incorrect.

1. When a subject establishes a conference call using a call conferencing service provided by the subscriber's carrier, it appears to be undisputed that communications over all legs of the call are "carried by the carrier * * * to or from the equipment, facilities, or services" of the subscriber, and therefore are covered by Section 103(a)(1), as long as the subject is "on the line." TIA asserts, however, that other legs of the call cease to be "carried * * * to or from the [subscriber's] equipment, facilities, or services" when the subject places other legs on hold or drops off the call. In essence, TIA argues that the conference call no longer uses the subscriber's "equipment, facilities, or services"

because the call content of the other legs is not being delivered from the switch to the subscriber's terminal. See TIA Comments at 32-33.

This argument reduces the subscriber's "equipment, facilities, or services" to nothing more than the local loop between the subscriber and the central office. That is, on its face, a wholly inadequate reading of the statutory language. As explained in the government's petition, a subscriber's "facilities" include all of the carrier's network components that support and are identifiable with the services associated with the subscriber's telephone number. See DOJ/FBI Petition ¶ 48 n.10. And the subscriber's "services" are all of the calling features and capabilities that the carrier makes available to the subscriber. A conference call initiated by the subscriber does not cease to use these "facilities" and "services" simply because the subscriber places the other legs of the call on hold or hangs up. If the other legs remain "up," it is only because the subscriber's services are providing that capability. And, needless to say, it is the subscriber who pays the carrier for the call conferencing capability that is being used and who pays any charges associated with the duration of the call itself -- demonstrating in practical terms that the subscriber's services are still involved.

TIA and other commenters argue that when communications between other parties to the conference call are not delivered to the subscriber's terminal, they are not being carried "to or from" the subscriber's equipment, facilities, or services. See, e.g., TIA Comments at 32-33. Here again, the commenters wrongly equate "facilities" and "services" with the subscriber's terminal and local loop. Unlike equipment, services are not physical objects and do not have a specific location. Hence, when the statute speaks of delivering communications "to or from" the subscriber's services, it is necessarily speaking in functional terms rather than physical or geographic ones: a communication is delivered "to or from" the subscriber's services when the carrier provides the services to carry out

the communication. Similarly, communications are "to or from" a subscriber's facilities when those facilities are used to carry the communications. Accordingly, Section 103(a)(1)'s "to or from" language offers no support for the interim standard.⁶

TIA's restrictive reading of Section 103(a)(1) is also at odds with CALEA's coverage of features like call forwarding. It is undisputed that if a subscriber has call forwarding capabilities, Section 103(a)(1) requires the carrier to have the capability to provide law enforcement with the content of forwarded calls. See House Report at 9, reprinted in 1994 USCCAN at 3489. Indeed, the interim standard itself expressly recognizes this requirement. See, e.g., J-STD-025 § 5.4.7 (Redirection message); id. Annex D, § D.11. Yet when a call is forwarded from the subscriber's number to another number, the resulting communication is not delivered to the subscriber's terminal, and the subscriber himself or herself need not be a party to the communication. Under the reading of Section 103(a)(1) advocated by TIA and other commenters, forwarded calls therefore would not be "to or from" the subscriber's equipment, facilities, or services. A reading of the statute that would lead to this result -- a result at odds with Congress's clear intent and the interim standard's own treatment of call forwarding -- is necessarily incomplete.

CDT suggests that Section 103(a)(1) is restricted to "the communications of the subscriber" -- meaning, apparently, communications in which the subscriber is taking part -- and therefore does not reach the communications of other parties when the subscriber is not on the line. CDT Petition at 40. This argument is squarely inconsistent with the language of Section 103(a)(1). By its terms,

⁶ TIA analogizes the delivery of communications between other conference call parties to the "transiting" of international calls across the United States. Ibid. Comparing the transiting of international calls with the operation of a subscriber's call conferencing services is, to be charitable, an apples-and-oranges comparison.

Section 103(a)(1) encompasses "all wire and electronic communications carried by the carrier * * * to or from equipment, facilities, or services of a subscriber * * * ." 47 U.S.C. § 1002(a)(1) (emphasis added). As long as a communication is carried "to or from [a subscriber's] equipment, facilities, or services," the carrier must make it available to law enforcement; the statute does not restrict that obligation to communications in which the subscriber (who, it should be recalled, might not even be a target of the criminal investigation) is participating.⁷

Several commenters suggest that, since law enforcement could not traditionally intercept the "held" portions of a conference call by monitoring the local loop (see DOJ/FBI Petition ¶ 51), such communications are therefore beyond the reach of Section 103(a)(1). See, e.g., AirTouch Comments at 9-10; BellSouth Comments at 8; SBC Comments at 9. As explained above, however, the traditional boundaries of law enforcement's surveillance capabilities are not dispositive. See pp. 10-11 supra. Where, as here, the express language of Section 103(a)(1) covers the communications in question, carriers are obligated to provide those communications, regardless of whether law enforcement could have acquired them through traditional monitoring techniques in the past.

AirTouch asserts that Section 107(b)(1) of CALEA, which calls for the Commission to adopt standards that "meet the assistance capability requirements of section 103 by cost-effective methods" (47 U.S.C. § 1006(b)(1)), requires the Commission to engage in a cost-benefit analysis to decide "whether the value of the capability * * * outweighs the costs carriers would incur in deploying the

⁷ CDT quotes a passage in the House Report which states that carriers must "ensure that new technologies and services do not hinder law enforcement access to the communications of a subscriber who is the subject of a court order." House Report at 16, reprinted in 1994 USCCAN at 3496. Nothing in this passage purports to limit the scope of Section 103(a)(1) to cases in which the subscriber is a party to the call, and the plain language of Section 103(a)(1) itself precludes any such limitation.

capability." AirTouch Comments at 13. This argument is fundamentally misconceived. Section 107(b)(1) merely directs the Commission to select cost-effective means of achieving the assistance capability requirements of Section 103; it does not permit, much less require, the Commission to dispense with those requirements. If Section 103(a)(1) encompasses the "held" portions of a subscriber's conference calls, then carriers are obligated to ensure that their networks can provide that information to law enforcement, absent a carrier-specific showing under Section 109(b) that compliance is not reasonably achievable, and any standards adopted by the Commission must ensure that that obligation is discharged in full.

Finally, several commenters suggest that the ability to monitor all legs of a conference call provided by the subscriber's local exchange carrier would be of little value to law enforcement, even if it were included in the interim standard, because a subject can conduct conference calls through conference bridge services provided by other carriers. See PrimeCo Comments at 10; AirTouch Comments at 14. This argument is misplaced for two reasons. First, the mere possibility that a subject may be able to evade authorized electronic surveillance does not excuse a carrier from its obligation under Section 103 to provide law enforcement with the capability to carry out the surveillance. Second, if a subject uses a conference bridge service provided by another carrier, law enforcement is free to seek a Title III order directed at the provider of the service. As a result, there is no gap in the coverage provided by Section 103.

2. In addition to arguments based on the language of CALEA, many commenters argue that CALEA does not require industry to provide law enforcement with the capability of intercepting conference calls in their entirety because Title III -- the statute that authorizes interceptions for surveillance purposes -- authorizes law enforcement to intercept conference calls only when the

intercept subject is "on the line." As we shall explain, however, Title III contains no such restriction. Accordingly, because CALEA requires that law enforcement be able to intercept "all wire and electronic communications * * * to or from equipment, facilities or services of a subscriber," the CALEA capabilities must include the ability to intercept the "held" portions of conference calls.

As explained in the government's petition, court orders issued under Title III are not directed towards individual people, but towards the telecommunications equipment, facilities, and services under surveillance. DOJ/FBI Petition at ¶ 48. A number of commenters nonetheless contend that law enforcement lacks authority under Title III to intercept the "held" portion of a conference call, either because the "subject" is no longer participating in the conversation (see, e.g., EPIC Comments at 23 n.67 (suggesting that law enforcement has "authority to monitor only the *subject's* conversation")), or because a target of the criminal investigation has left the call (see, e.g., CDT Comments at 38 (contending that "the purpose of CALEA was to follow the target")), or both (see BellSouth Comments at 8 (stating that "it is the communications content of the specific target, or subject, of the authorized electronic surveillance which is at issue")). These commenters generally appear to assume, erroneously, that some person targeted or identified by law enforcement in

connection with the wiretap must participate in any conversation that can properly be intercepted.⁸

We briefly set forth the correct legal principles here.

A Title III application and order focus upon the nexus between a criminal offense and telecommunications facilities that are likely to lead to information about that offense. Before entering an interception order under Title III, a judge must find that there is probable cause to believe both that "an individual" is committing, or is about to commit, a criminal offense (18 U.S.C. § 2518(3)(a)), and that "the facilities from which * * * communications are to be intercepted are being used, or are about to be used, in connection with the commission of such offense, or are leased to, listed in the name of, or commonly used by such person." 18 U.S.C. § 2518(3)(d) (emphasis added).⁹ Accordingly, an interception order under Title III must specify "the identity of the person, if known, whose communications are to be intercepted" (18 U.S.C. § 2518(4)(a) (emphasis added)), a description of "the type of communication sought to be intercepted, and a statement of the particular offense to which it relates" (18 U.S.C. § 2518(4)(c)), and "the nature and location of the communications facilities as to which * * * authority to intercept is granted" (18 U.S.C. §

⁸ Some of the commenters' confusion stems from the Interim Standard's definition of a "subject" as "a telecommunications service subscriber whose communications, call-identifying information, or both, have been authorized by a court to be intercepted." J-STD-025 at 1. The Interim Standard's definition is inadequate because, as we explain below, almost all court orders authorize the interception of calls to particular facilities, rather than to particular people. As defined in the Interim Standard, therefore, the term "subject" lacks a referent except in the unusual case of a "roving" wiretap. This Reply Comment uses the definitions of the terms "subscriber" and "subject" set forth in the government's rulemaking petition: a "subscriber" is the person or entity whose equipment, facilities, or services are the subject of an authorized law enforcement surveillance activity, while a "subject" is any person who is using the subscriber's equipment, facilities, or services. DOJ/FBI Pet. ¶ 47; see also id. Appendix 1, at 3 (defining "subject" and "subscriber").

⁹ The judge must also find that intercepted communications would concern the offense, and that normal investigative techniques are inadequate. 18 U.S.C. §§ 2518(3)(b) and (c).

2518(4)(b)). The statute therefore cannot be interpreted to provide that a Title III order is directed solely to the interception of a particular individual's conversations, whether that person is the target of a criminal investigation or the subscriber to a particular telephone line. On the contrary, the order authorizes the interception of communications that take place over specific telecommunications facilities and relate to a particular criminal offense -- the identity of individual speakers need be specified only "if known."

In light of this statutory scheme, the Supreme Court has specifically held that a Title III order authorizes law enforcement to intercept a conversation that takes place over facilities subject to an interception order even if none of the parties to the conversation is named in the order itself. United States v. Kahn, 415 U.S. 143 (1974).¹⁰ The Supreme Court in Kahn recognized that "when there is probable cause to believe that a particular telephone is being used to commit an offense but no particular person is identifiable, a wire interception order may, nonetheless, properly issue under the statute."¹¹ 415 U.S. at 157. The Court explained that interception orders frequently seek to

¹⁰ TIA suggests that Kahn implies that "Section 2518 only authorizes law enforcement access to communications that can be heard over the targeted facilities." TIA Comments at 37. This contention is obviously wrong, because the statute now expressly provides for the interception of "electronic communications," defined as "any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature." 18 U.S.C. § 2510(12) (added in 1986 as part of the Electronic Communications Privacy Act). Moreover, the statute defines "interception" as "the aural or other acquisition" of communications. 18 U.S.C. § 2510(4).

¹¹ AirTouch incorrectly cites the Supreme Court's decision in United States v. Donovan, 429 U.S. 413 (1977), for the proposition that Title III orders that fail to name individuals violate the Fourth Amendment's particularity requirement. AirTouch Comments at 11 n.36. But Donovan holds, in the very passage from the opinion that AirTouch quotes, that "a wiretap application must name an individual if the Government has probable cause to believe that the individual is engaged in criminal activity." Donovan, 429 U.S. at 428 (emphasis added). To the extent that the government has probable cause to believe that the facilities are being used to commit an offense, but lacks probable cause with regard to a particular individual, there is no constitutional or statutory

(continued...)

identify individuals who are involved in criminal activity but who are unknown to law enforcement. See *id.* at 156-157. Interception orders serve the same investigatory purpose today. See Joint Hearings at 18 (prepared statement of FBI Director Freeh) ("Electronic surveillance is critical in the monitoring of drug traffickers' 'communications networks,' providing law enforcement with the ability to identify all of the organization's drug traffickers and their illegal proceeds").

Many commenters seem to assume that the individual who sets up the conference call and whose facilities are under surveillance must invariably have some connection with criminal activity. See, e.g., CDT Comments at 38 (stating that the FBI's concern is to "listen to the communications of a target"); SBC Comments at 8-9 (complaining that law enforcement seeks to intercept communications "regardless of whether or not the target party, *i.e.* the party named in the court order, is actually on the line"); EPIC Comments at 23 n.67 (claiming that "law enforcement with authority to monitor only the *subject's* conversation is not permitted to trace conversations on the facilities once the subscriber disconnects") (underlining added). But there is no basis for such an assumption -- on the contrary, Title III expressly contemplates that telecommunications facilities are subject to surveillance when they "are being used, or are about to be used, in connection with the commission of" a criminal offense, without regard to the identity or possible culpability of the subscriber. Indeed, an innocent subscriber might well set up a conference call for two targets of a criminal investigation, both named in an order that authorized interception of communications carried on the subscriber's facilities. Under the commenters' view of Title III, law enforcement would be authorized to monitor only those portions of the conference call in which the subscriber

¹¹(...continued)
requirement that the individual be named.

participated, and would be barred from intercepting any conversations that took place between the two suspected criminals while the subscriber was on hold, or had left the conversation permanently. Indeed, the same would be true for non-conference calls -- if a drug dealer's girlfriend called a confederate from her (tapped) telephone, gave the handset to her boyfriend and left the house, then, under the commenters' mistaken view of Title III, law enforcement would be unable to monitor the call. Title III, however, expressly authorizes interception under such circumstances.

There is therefore no legal basis for the commenters' claim that law enforcement lacks statutory authority to intercept the "held" portions of conference calls if a "subject" who was a party to an earlier portion of the conversation is no longer a participant. On the contrary, law enforcement's interception authority under Title III extends to all conversations that can be intercepted through the specified telecommunications facilities, regardless of the identity of the speakers. Much of the opposition on this point is thus based upon a misperception of Title III law.¹²

Unlike many other commenters, TIA properly acknowledges that Title III "allows interception of communications by persons other than intercept subject[s] who use the facilities of the intercept subject." TIA Comments at 34-35. However, TIA maintains that Title III nonetheless does not permit law enforcement to intercept the "held" portions of conference calls because to do so "would effect a huge expansion of the facilities doctrine." *Ibid.* According to TIA, the "facilities doctrine" is "limited by the requirement that the intercept involve the actual telephone or other

¹² One commenter argues that access to the "held" portions of conference calls "is specifically denied by 103(a)(4) of CALEA." ATR Comments at 18. Section 103(a)(4), however, merely requires carriers to perform interceptions in a manner that protects "the privacy and security of communications * * * not authorized to be intercepted." Nothing in Section 103(a)(4) purports to narrow the scope of law enforcement's interception authority -- rather, the statute imposes requirements regarding communications that are not subject to interception under existing authority.

physical facilities of the intercept subject -- as opposed to the entire system or network to which the telephones are attached." Ibid. TIA is factually mistaken in asserting that law enforcement seeks the capacity to intercept the calls carried over an "entire system or network"; moreover, its legal analysis is wrong as well.

The "facilities" at issue here are telecommunications facilities that carry "wire, oral or electronic communication[s]." 18 U.S.C. § 2518(1). As we have explained, the purpose of Title III is to authorize the interception of calls carried on specific telecommunications facilities if there is probable cause to believe that such calls will include "particular communications concerning [a specified criminal] offense." 18 U.S.C. § 2518(3)(a). Obviously, Title III cannot be read in a manner that causes changes in technology to render it obsolete. Restricting "facilities" under Title III to specific physical equipment such as the subscriber's local loop, or even the physical components of a carrier's switch, would greatly undermine the statute's effectiveness in the current telecommunications universe, and would frustrate Congress's purpose in giving interception authority to law enforcement. Instead, the term "facilities" must be understood functionally, just as it always has been, as the "communications pathway" where the communications are to be intercepted, regardless of where that pathway may physically be found. DOJ/FBI Petition at 28 n.10.¹³

¹³ TIA suggests that unless the term "facilities" refers to a particular telephone, Title III would violate the Fourth Amendment requirement of particularity. TIA Comments at 36 n. 86. But TIA goes on to rebut its own argument, conceding that this proposition would be true only to the extent that the intercepted call "does not involve any facilities identifiable with the subscriber." Ibid. Of course, any possible interpretation of "facilities" under Title III must link the communications facilities to the subscriber, and it makes no sense to suggest that only a definition that equates "facilities" with "particular telephone" could demonstrate the requisite degree of connection.

Moreover, TIA's reliance upon United States v. Tavaréz, 43 F.3d 1136 (10th Cir. 1994) is
(continued...)

As a matter of historical fact, it is generally true that the telecommunications facilities for which interception authority was granted were associated with fixed, physical equipment, usually the subscriber's local loop.¹⁴ See also CDT Comments at 39 (arguing that "facilities" "has a physical connotation"). Congress enacted CALEA, however, precisely because advances in telecommunications technology had greatly reduced the value of interceptions made at the level of the local loop, and Congress wanted to "preserve the government's ability, pursuant to court order, to intercept communications that utilize advanced technologies." House Report at 16. The FBI Director had explained to Congress that new multiplexing capabilities, coupled with advanced communications services and features, "undermine the necessity for communications to be transmitted always to the same specific location or through the same wireline loop." *Ibid.*¹⁵ Indeed, the deployment of sophisticated digital technology generally disassociates a telephone subscriber's communications facilities from particular pieces of physical equipment, because functions that were formerly performed by dedicated hardware are now performed by software that employs whatever

¹³(...continued)

misplaced. See TIA Comments at 35 n. 80. The court in Tavarez explicitly based its holding upon the language of the state statute that formed the basis for the interception at issue. See 43 F.3d at 1139 ("usage of the term ["facilities"] in other provisions of the Oklahoma Act indicates that "facilities" means target telephones * * * "facilities" is used elsewhere in the Oklahoma Act to mean the targeted telephones").

¹⁴ "[T]raditionally, common carriers have offered essentially 'fixed point' telecommunications * * * transmitted over common carrier facilities, such as telephone wires that were dedicated to a customer's specific telephone number (often referred to as a subscriber's 'loop')." Joint Hearings at 24 (prepared statement of Louis J. Freeh).

¹⁵ See also Joint Hearings at 43 (Responses of Louis J. Freeh to Questions Submitted by Senator Leahy) ("As the features and services being deployed and offered by service providers have become more advanced, the communications and dialing information that law enforcement agencies attempt to intercept and acquire become less accessible in the local loop, *and* effective central office access has not been developed by the telephone companies").

hardware may be available at least cost to the system. See John Bellamy, Digital Telephony at 441 (2d ed. 1991) (describing virtual circuit networks and explaining that "a virtual circuit is a logical concept involving addresses and pointers in the nodes of the network, but no dedicated transmission facilities").

Congress understood these concerns when it enacted CALEA. Congress did not specify in CALEA that the telecommunications industry must preserve law enforcement's interception capabilities by routing all calls through the local loop. Rather, Congress encouraged industry to implement new technologies, but required carriers to develop and deploy the capability for allowing law enforcement to intercept, "pursuant to a court order or other lawful authorization, * * * all wire and electronic communications carried by the carrier within a service area to or from equipment, facilities or services of a subscriber of such services." CALEA, § 103(a)(1). Thus, Congress did not allow technological changes to have the effect of limiting law enforcement's existing interception authority under Title III; rather, it took steps to ensure that advanced telecommunications systems would retain the capability to deliver meaningful interceptions within the well-established scope of that authority. See House Report at 10 (stating that "[t]he purpose of [CALEA] is to preserve the government's ability, pursuant to court order or other lawful authorization, to intercept communications using advanced technologies such as digital or wireless transmission modes, speed dialing and conference calling"). Contrary to the commenters' assertions, therefore, the capabilities mandated by CALEA include the ability to intercept conference calls in their entirety, even if the subscriber puts other parties to the call on hold or leaves the call altogether, and Title III permits law enforcement to intercept every leg of a call carried "to or from the

equipment, facilities or services" of the subscriber, regardless of whether the subscriber is on the line.

B. The Scope of "Call-Identifying Information"

1. We now turn from Section 103(a)(1) of CALEA, which concerns the interception of communications, to Section 103(a)(2), which concerns access to "call-identifying information." A number of the capabilities missing from the interim standard involve the failure to ensure law enforcement's access to call-identifying information. CALEA specifically defines "call-identifying information" as "dialing or signaling information that identifies the origin, direction, destination, or termination of each communication generated or received by a subscriber by means of any equipment, facility, or service of a telecommunications carrier." 47 U.S.C. § 1001(2). The government's petition explains why each of the capabilities in question involves "call-identifying information" within the scope of this statutory definition.

Beginning at a relatively early stage in the standard-setting process, industry adopted its own, highly restrictive, definition of "call-identifying information," a definition that is now part of the interim standard. See J-STD-025 § 3. The industry definition forms the basis for many of the arguments by TIA and other commenters regarding the assistance capabilities in the government's petition. However, industry's definition is deeply flawed and fundamentally inconsistent with CALEA's underlying goal of "preserv[ing] the government's ability" to carry out legally authorized electronic surveillance. House Report at 9, reprinted in 1994 USCCAN at 3489. Therefore, before

we address particular assistance capabilities involving call-identifying information, we first discuss why industry's definition of "call-identifying information" is incorrect.¹⁶

To understand the scope of "call-identifying information," the legislative history surrounding the term must be reviewed. The original draft of the bill that evolved into CALEA did not use the term "call-identifying information" at all. Instead, it referred to "call setup information." See Joint Hearings at 267-68. "Call setup information" was defined in the draft bill as "the information generated which identifies the origin and destination of a wire or electronic communication placed to, or received by, the facility or service that is the subject of the court order or lawful authorization, including information associated with any telecommunication system dialing or calling features or services." Ibid.

During the course of the legislative process, Congress replaced "call setup information" with "call-identifying information." In doing so, Congress not only changed the operative term, but also clarified and expanded the scope of the statutory definition. As defined in CALEA, "call-identifying information" explicitly covers both dialing information and signaling information. 47 U.S.C. § 1001(2).¹⁷ Moreover, while "call setup information" was confined to information identifying the

¹⁶ Law enforcement specifically objected to the language of industry's definition during the standard-setting process (see DOJ/FBI Petition, Appendix 3, p. 2), and the government has omitted industry's definition from the proposed rule that accompanies the government's rulemaking petition. To the extent that TIA seems to suggest that the government has not taken issue with the industry definition (see TIA Comments at 38), it therefore is simply wrong.

¹⁷ CDT attempts to read "signaling information" out of the statutory definition. See CDT Comments at 22-24. CDT asserts that signaling information "includes nothing beyond 'dialing' information" and that signaling is "coextensive" with "dialing." Id. at 22-23. This reading of the statutory definition renders "signaling information" redundant. It therefore conflicts with the elementary principle that "legislative enactments should not be construed to render their provisions mere surplusage." Dunn v. CTEFC, 117 S. Ct. 913, 917 (1997); Bennett v. Spear, 117 S. Ct. 1154, (continued...)

"origin" and "destination" of communications, "call-identifying information" includes not only "origin" and "destination," but the "direction" and "termination" of communications as well. Ibid.¹⁸

The definition of "call-identifying information" employed in the interim standard effectively disregards the changes that Congress made when it replaced "call setup information" with "call-identifying information." In particular, the industry definition deprives "direction" and "termination" of their intended scope. The interim standard defines "direction" as "the number to which a call is re-directed or the number from which it came, either incoming or outgoing (e.g., redirected-to party or redirected-from party)." Information identifying redirected-to and redirected-from parties, however, was already encompassed within "origin" and "destination." Moreover, by focusing exclusively on redirected-to and redirected-from parties, the interim standard effectively turns "direction" into "redirection." Similarly, the interim standard defines "termination" as "the number of the party ultimately receiving a call (e.g., answering party)," yet "destination" was sufficient to capture that information. If Congress had intended to cover only the information identified in the interim standard, it would not have had to add "direction" and "termination" to the statutory definition at all. The interim standard thus comes perilously close to reading "direction" and "termination" out of the statute.

¹⁷(...continued)

1167 (1997) ("[i]t is our duty to give effect, if possible, to every clause and word of a statute") (internal quotation marks omitted).

¹⁸ CDT asserts that Congress intended for "call-identifying information" to have the same meaning as "call setup information." See CDT Comments at 25-26. If that had been Congress's intent, Congress would not have had to change the term in the first place, much less revise the statutory definition of the term.

The industry definition also results in the exclusion of a wide range of dialing and signaling information to which law enforcement traditionally has had access in the POTS environment. As explained in the petition, law enforcement traditionally has been able to capture all of the dialing and signaling information used for call processing that traverses the "local loop" between the subscriber and the central office. Thus, for example, law enforcement could detect tones and signaling information indicating call waiting, a conference call, or the transfer of a call. DOJ/FBI Petition ¶ 58. Similarly, law enforcement could detect signaling information indicating how the network treated a call attempt, such as ringing or a busy tone. *Id.* ¶ 81. These kinds of information have substantial investigatory and evidentiary value for law enforcement. Nevertheless, the industry definition purports to exclude this kind of dialing and signaling information from the scope of Section 103 altogether.

As noted above, we do not contend that law enforcement's traditional electronic surveillance capabilities are dispositive regarding the reach of CALEA. See pp. 10-11 *supra*. But at the very least, the Commission should not assume that Congress intended to narrow the scope of law enforcement's capabilities in this fashion without compelling evidence of such a purpose. No such evidence has been presented.

Several commenters point to a passage in the House Report that states that, "[f]or voice communications, [call-identifying] information is typically the electronic pulses, audio tones, or signaling messages that identify the numbers dialed or otherwise transmitted for the purpose of routing calls through the telecommunications carrier's network." House Report at 21, reprinted in 1994 USCCAN 3501 (emphasis added). As the use of the word "typically" indicates, however, this

passage is meant to provide only an illustration, not a definition, of "call-identifying information."¹⁹

In the balance of the passage, the House Report states that "[o]ther dialing tones * * * that are used to signal customer premises equipment of the recipient are not to be treated as call-identifying information." *Ibid.* (emphasis added). If the language relied on by the commenters had been intended as an exhaustive definition of "call-identifying information," as the commenters suggest, Congress would have had no reason to include the underscored language; rather, it would have said without qualification that no other dialing or signaling tones constitute call-identifying information.

The government's rulemaking petition rests on a less crabbed reading of the statutory language than the one employed in the interim standard. In particular, the government's petition employs a more natural and logical reading of "direction" and "termination."²⁰

Read naturally, "information identifying * * * the direction" of a communication encompasses not only information about the path of the communication through a network, but also information about any dialing and signaling activity by the subscriber that directs the communication. For example, when the subscriber presses a flash hook or feature key to transfer or forward the call, he

¹⁹ The illustrative, non-comprehensive nature of the passage is further indicated by the fact that it refers only to the "origin" and "destination" of communications, while the statutory definition of call-identifying information also includes "direction" and "termination." Compare House Report at 21, reprinted in 1994 USCCAN at 3501 (call-identifying information "identifies the origin and destination of a wire or electronic communication"), with 47 U.S.C. § 1001(2) (call-identifying information means information "that identifies the origin, direction, destination, or termination of each communication * * *").

²⁰ Although our discussion here focuses principally on "direction" and "termination," the interim standard's definitions of "origin" and "destination" are likewise unduly restrictive. The interim standard defines "origin" as "the number of the party initiating a call" and "destination" as "the number of the party to which a call is being made (e.g. called party)." These definitions exclude obvious call-identifying information, such as temporary local directory numbers for mobile call routing and routing numbers for ported calls.

is engaged in directing the call. Carriers therefore are obligated under Section 103(a)(2) to provide a message that identifies such instances of call direction.

As for "termination," a call attempt may "terminate" in a variety of ways: with an answer by the called party, with ringing (without an answer), with a busy tone or a trunk busy signal, with automatic redirection to a voice mail box, or in other ways. "Information identifying * * * the termination" of a communication therefore encompasses not only the number of the answering party, but also information perceived by the subject about how the call terminated -- information reflected, for example, by busy tones or "stutter" dial tones. All such signaling information comes within the statutory definition of "call-identifying information."

When "call-identifying information" is read in this common-sense manner, law enforcement's traditional capabilities regarding the acquisition of dialing and signaling information are preserved rather than impaired. And when the corresponding shortcomings in industry's restrictive definition of "call-identifying information" are kept in mind, a large share of the commenters' objections to the government's petition fall away.

2. CALEA requires a carrier to provide access to all call-identifying information that is "reasonably available to the carrier * * * ." 47 U.S.C. 1002(a)(2). A number of commenters assert that, for one reason or another, particular dialing and signaling information sought in the government's petition is not "reasonably available" and that the interim standard is therefore not deficient in failing to require delivery of such information. See, e.g., Nextel Comments at 11; USTA Comments at 5; PrimeCo Comments at 14; CDT Comments at 43.

To the extent that these comments are directed at particular types of call-identifying information, we address them individually in the relevant sections of the discussion below. However, three points regarding the general issue of "reasonable availability" should be made at the outset.

First, we strongly disagree with those commenters who suggest that the potential cost of delivering particular call-identifying information to law enforcement is, by itself, a basis for deeming the information "not reasonably available." Congress understood that compliance with Section 103's assistance capability requirements might be prohibitively expensive in particular cases. But there is no indication that Congress meant for the "reasonably available" language of Section 103(a)(2) to deal with that problem. Instead, Congress provided for relief under Section 109(b) of CALEA, which excuses carriers from meeting assistance capability requirements that are not "reasonably achievable" with respect to particular equipment, facilities, and services unless the government pays the additional reasonable costs of compliance. See 47 U.S.C. § 1008(b). The statutory standards for "reasonable achievability" under Section 109(b) expressly incorporate cost concerns. See *id.* § 1008(b)(1)(B), (D), (E), (H). In contrast, there is nothing in the language or legislative history of Section 103(a)(2) that suggests that Congress intended for cost considerations to govern the underlying scope of carriers' assistance capability obligations. Issues of "reasonable availability" under Section 103(a)(2) should focus on technical issues rather than the kinds of financial issues that are addressed in Section 109(b) and elsewhere in CALEA.²¹

²¹ Several commenters note that the government recently has received CALEA cost estimates from manufacturers and shortly will present Congress with an implementation report that discusses cost issues. See AirTouch Comments at 5; US West Comments at 22, 26. The proprietary information provided by manufacturers is subject to non-disclosure agreements (NDAs) that severely limit the ability of the government to disclose cost data. To the extent that the implementation report discusses cost issues, it does so in aggregate terms that do not discuss the
(continued...)

Second, the commenters are wrong when they suggest that call-identifying information should not be regarded as "reasonably available" unless there is a "business purpose" for making such information available." TIA Comments at 39 (emphasis added); Nextel Comments at 11. "Business purpose" can hardly be the touchstone for analysis under Section 103. Congress imposed the assistance capability requirements of Section 103 precisely because carriers following the dictates of "business purposes" cannot be expected to provide law enforcement with the kind of assistance that is needed to perform authorized electronic surveillance. By virtue of CALEA, "telecommunications carriers * * * are [now] required to design and build their switching and transmission systems to comply with the legislated requirements." House Report at 18, reprinted in 1994 USCCAN at 3498 (emphasis added). Whether providing particular information serves a "business purpose" of the carrier is simply irrelevant to whether the carrier must incorporate the delivery of such information to law enforcement in the design of its network.

Third, questions of "reasonable availability" do not necessarily lend themselves to generic, across-the-board answers. Delivering particular call-identifying information to law enforcement may be technically straightforward with respect to one platform or network architecture and considerably more difficult and complex with respect to another. Thus, particular call-identifying information may prove to be "reasonably available" to one carrier and not "reasonably available" to another.

²¹(...continued)

costs associated with individual "punch list" items. Even the aggregated cost information in the implementation report is subject to NDA limitations and is being provided to Congress only with the express permission of the manufacturers involved. If the manufacturers are willing to grant written permission with respect to the Commission, the government would accede to their request and provide a copy of the report to the Commission.

The Commission does not have to establish that particular call-identifying information is "reasonably available" to all carriers in all circumstances in order for such information to be included in standards issued under Section 107(b). As explained above, standards issued by the Commission are simply a safe harbor; no carrier is legally obligated to use the means set forth by the Commission if it believes that it can satisfy its underlying assistance capability obligations under Section 103 in another manner. See pp. 13-14 supra. As a result, the Commission does not have to dilute its standards to account for the possibility that call-identifying information that is "reasonably available" for some carriers may not be "reasonably available" for all.

At the same time, an assertion that particular call-identifying information is not "reasonably available" with respect to particular platforms is not sufficient, even if true, to show that the interim standard is not "deficient." As explained above, by virtue of CALEA's safe-harbor provision, the interim standard effectively displaces the underlying assistance capability requirements of Section 103 for carriers that implement the interim standard. See pp. 12-13 supra. If particular call-identifying information is "reasonably available" to some of the carriers covered by the interim standard, the failure of the interim standard to include such information renders the interim standard deficient, regardless of whether the same information is equally available to other carriers.

C. Post-Cut-Through Dialing

1. The first capability concerning call-identifying information that is missing from the interim standard is the delivery of "post-cut-through" dialed digits. As explained in the government's petition, post-cut-through dialing is used in long distance calls, credit card calls, and (in some instances) local calls to complete the call and reach the intended party. DOJ/FBI Petition ¶ 66. For reasons set forth in the petition, post-cut-through dialing used to complete calls has important

investigatory and evidentiary value to law enforcement. Id. ¶¶ 68-71. Post-cut-through dialing and signaling information that completes a call is "dialing or signaling information" that identifies the "destination" of the call, placing it directly within CALEA's definition of "call-identifying information" (47 U.S.C. § 1001(2)). Id. ¶ 69. As a result, the interim standard's failure to require delivery of post-cut-through dialing used to complete calls renders the standard deficient.

In response to the government's petition, many of the commenters point out that a subscriber may engage in post-cut-through dialing for purposes other than call completion. In particular, a subscriber may dial digits after the cut-through in order to control or otherwise interact with equipment of the called party. For example, a subscriber might enter a PIN number to access his bank account information, or he might make numeric selections from a voice-mail menu to access other kinds of information.

We readily acknowledge that, in some instances, post-cut-through digits are dialed for purposes other than call completion and do not represent the number of a called party. In those instances, we do not contend that the post-cut-through digits constitute "call-identifying information." But when post-cut-through digits are dialed for call completion, they "identif[y] the * * * destination * * * of [a] communication" and therefore come squarely with the statutory definition of "call-identifying information."

The legislative history of CALEA reflects this distinction. As noted above, the House Report's discussion of call-identifying information states that "[o]ther dialing tones that may be generated by the sender that are used to signal customer premises equipment of the recipient are not to be treated as call-identifying information." House Report at 21, reprinted in 1994 USCCAN at 3501 (emphasis added). As the underscored language shows, Congress did not exclude post-cut-

through dialing from the scope of "call-identifying information" altogether; it simply indicated that post-cut-through dialing is excluded when it is "used to signal customer premises equipment of the recipient." The testimony of the FBI Director reflects the same distinction. See, e.g., Joint Hearings at 50 ("What I want with respect to pen registers is the dialing information"; "[a]s to the banking accounts and what movies someone is ordering at Blockbuster, I do not want it [and] do not need it" under pen register authority). Contrary to the suggestion of some of the commenters (e.g., CDT Comments at 42-43; AT&T Comments at 8-9), nothing in the legislative history even remotely suggests that Congress intended to treat post-cut-through dialing used for call completion as anything other than "call-identifying information."

Several commenters argue that because post-cut-through dialing is not always call-identifying information, carriers are not obligated to provide access to post-cut-through dialing at all. See, e.g., TIA Comments at 45-46; CDT Comments at 43. They base this argument on Section 103(a)(4)(A) of CALEA, which directs carriers to assist law enforcement surveillance activities "in a manner that protects * * * the privacy and security of communications and call-identifying information not authorized to be intercepted * * * ." 47 U.S.C. § 1002(a)(4)(A). They argue that Section 103(a)(4)(A) prohibits carriers from giving law enforcement post-cut-through digits that are not involved in call completion. Because carriers currently lack any technological means to discriminate between post-cut-through digits dialed for call completion and digits dialed for transactional purposes, the commenters reason that the only way for carriers to comply with Section 103(a)(4)(A) is not to provide post-cut-through digits at all.

The short answer to this argument is that Section 103(a)(4)(A) has nothing to do with the issue of post-cut-through dialing. Congress understood that pen register surveillance could result in

the delivery of transactional dialing information, but it dealt with that problem through Section 207 of CALEA, not Section 103(a)(4)(A). See House Report at 31-32, reprinted in 1994 USCCAN at 3511-12. Section 207, now codified as 18 U.S.C. § 3121(c), provides that a law enforcement agency using pen registers "shall use technology reasonably available to it that restricts the recording or decoding of electronic or other impulses to the dialing and signaling information utilized in call processing." Section 207 presupposes that carriers will deliver transactional data to law enforcement in the course of carrying out pen register orders. Rather than prohibit carriers from doing so, Congress instead chose to impose a technology-based minimization obligation on law enforcement.²²

Some commenters argue that the interim standard is not deficient because law enforcement can obtain post-cut-through dialed digits as part of call content by serving the subscriber's local carrier with a Title III order. See TIA Comments at 42-43; PrimeCo Comments at 13. But when a subscriber dials post-cut-through digits to complete a call, the dialed digits are call-identifying information, not call content, and law enforcement is entitled to acquire them with a pen register order. Forcing law enforcement to meet the heightened requirements of Title III in order to acquire post-cut-through digits is therefore inconsistent both with CALEA and with the structure of the underlying electronic surveillance statutes.²³

²² Even taken on its own terms, without regard to Section 207, the commenters' reliance on Section 103(a)(4)(A) is misplaced. Section 103(a)(4)(A) does not purport to override a carrier's unqualified obligation under Section 103(a)(2) to provide access to reasonably available call-identifying information. A carrier therefore cannot invoke Section 103(a)(4)(A) as a "defense" to its failure to meet its obligations under Section 103(a)(2).

²³ TIA asserts that post-cut-through dialed digits are not call-identifying information "for the initial carrier." TIA Comments at 44. But neither the statutory definition of "call-identifying information" nor the statutory obligation to provide access to call-identifying information is tied to whether "the initial carrier," as opposed to another carrier, uses the digits to complete the call. See (continued...)

Alternatively, some commenters suggest that law enforcement can obtain post-cut-through digits by serving a pen register order or a subpoena on the carrier that provides the long distance service. See TIA Comments at 42; CDT Comments at 42. This argument is both legally and practically misconceived. As a legal matter, nothing in Section 103(a)(2) relieves a carrier of its obligation to "expeditiously isolat[e] and enabl[e] the government * * * to access call-identifying information" when the information is (or is claimed to be) available from another source. As a practical matter, the "solution" of turning to the long-distance carrier is no solution at all. Thousands of carriers provide long-distance calling card and credit card services; a subject can choose from among all of them and may change from one to another with each successive call. Law enforcement cannot possibly determine which particular long-distance provider is being used by the subject for a particular call and acquire the dialed digits sent to the provider in anything like real time. Congress understood that law enforcement needs to acquire call-identifying information contemporaneously with the calls to which it relates; it is for that reason that Section 103(a)(2) obligates carriers to provide call-identifying information "expeditiously" and "before, during, or immediately after" the transmission of the associated communication. Serving a long-distance carrier with a subpoena to get post-cut-through digits from billing records is patently inadequate to meet the law enforcement needs that Congress acknowledged and incorporated into Section 103(a)(2).²⁴

²³(...continued)

47 U.S.C. §§ 1001(2), 1002(a)(2).

²⁴ The problem is particularly acute when prepaid calling cards are used. A long-distance provider has no need to keep track of who is using a prepaid calling card; it merely debits the account associated with the card as long-distance calls are made. When a subject uses a prepaid card, law enforcement therefore could not obtain the desired dialing information from the provider at all unless law enforcement somehow knew the account number of the card that the subject was using. In some
(continued...)

Finally, a number of commenters assert that post-cut-through dialed digits are not "reasonably available" to local carriers because detecting them would require potentially expensive modifications of existing equipment. See TIA Comments at 44-45; USTA Comments at 7; Ameritech Comments at 6-7; BellSouth Comments at 15; PrimeCo Comments at 13. To capture post-cut-through digits for delivery to law enforcement, a carrier may apply a tone decoder to the call or detect the dialed digits outside the switch by a "loop-around" or other means.²⁵ The commenters note that tone decoders are shared resources, which ordinarily are freed for use on other calls after a particular call has been cut through; in order to detect dialed digits after cut-through, a tone decoder will have to be dedicated to the call content channel for the duration of the call. The commenters add that some technologies (such as cellular and PCS) may not currently be configured to detect touch tones at all and therefore will have to add this capability. See BellSouth Comments at 15; USTA Comments at 7.²⁶

²⁴(...continued)

cases, moreover, long-distance providers do not even maintain records of the number being called. Since the rate per minute for calls made with prepaid calling cards is usually fixed and does not depend on the distance between the calling and called parties, a long distance carrier may have no need to maintain a record of the called number for billing purposes.

²⁵ We note that the current Signaling System 7 (SS7) protocol already has an option to have the number of the answering party returned as part of the SS7 Answer message. This option has not been deployed in the United States, but it has been deployed in several other parts of the world. If it were deployed here, the local carrier would be able to determine post-cut-through digits used for call completion without any need to monitor the post-cut-through data stream itself.

²⁶ TIA states that delivery of post-cut-through digits would be especially difficult when a subscriber uses a "voice recognition dialing" feature (a feature that allows the subscriber to designate a called party by saying the party's name or other identifying word rather than by dialing the number). TIA Comments at 45. The government's petition does not seek the delivery of the translated digits generated by voice recognition dialing unless the carrier (or a provider of telecommunications support services under the carrier's control) is the one performing the translation. Thus, in the typical post-
(continued...)

It is certainly true that carrier equipment will have to be modified in order to detect and extract post-cut-through digits. However, neither that fact nor the potential expense of the modifications means that the information is not "reasonably available." Congress understood that telecommunications carriers would be "required to design and build their switching and transmission systems to comply with the legislated requirements" of CALEA. House Report at 18, reprinted in 1994 USCCAN at 3498. As explained above, the costs associated with system modifications are appropriately dealt with through the reimbursement provisions of Section 109(b), not the assistance capability requirements of Section 103. See p. 36 supra. If "the total cost of compliance is wholly out of proportion to the usefulness of achieving compliance for a particular type or category of services or features" (House Report at 28, reprinted in 1994 USCCAN at 3508), relief is available under Section 109(b). Otherwise, the cost of implementation should not excuse carriers from providing what is unquestionably call-identifying information.

2. The government's proposed rule provides for post-cut-through dialed digits to be delivered to law enforcement on a call data channel rather than a call content channel. DOJ/FBI Petition, Appendix 1 (§ 64.1708(i)(1)). The proposed rule contains a similar provision regarding the delivery of notification messages for network-generated in-band and out-of-band signaling (see pp. 55-59 infra). Id. § 64.108(d).

TIA argues that the failure to provide this information on a call data channel does not render the interim standard "deficient" and that the Commission therefore cannot include such a requirement

²⁶(...continued)

cut-through case where the voice recognition dialing feature is implemented by a long-distance carrier, the local carrier would be under no obligation to provide access to the translated digits (or the actual words spoken to use the feature).

in its standards. TIA Comments at 61-62. As noted in the government's rulemaking petition, we agree that a carrier can satisfy its assistance capability obligations under Section 103 without necessarily delivering such information on a call data channel. See DOJ/FBI Petition ¶ 84. However, it does not follow that the Commission is powerless to address this issue as part of the present proceeding.

As explained above, the interim standard does not require the delivery of post-cut-through dialed digits at all. That omission renders the interim standard deficient and thereby triggers the Commission's authority under Section 107(b). Once the Commission is authorized to act under Section 107(b), it may take a variety of considerations into account in framing an appropriate standard. See 47 U.S.C. § 1006(b)(1)-(5). Among other things, the Commission may consider the cost-effectiveness and privacy impact of alternative solutions. Id. § 1006(b)(1), 1006(b)(2).

As explained in the government's petition, requiring the government to use both a call data channel and a call content channel when it is engaged in pen register surveillance results in needless duplication of equipment, facilities, and cost. DOJ/FBI Petition ¶ 84. In addition, delivery of post-cut-through digits to law enforcement over a call content channel creates an unnecessary risk of inadvertent intrusions on call content when the government is seeking (and is specifically authorized to seek) only call-identifying information. Id. ¶ 85. For these reasons, if the Commission agrees that Section 103(a)(2) obligates carriers to provide law enforcement with post-cut-through digits, the Commission appropriately may include the use of a call data channel for the delivery of such information in the Commission's standards.²⁷

²⁷ TIA suggests that delivery of post-cut-through digits over the call data channel is a new request that was not part of law enforcement's "punch list." That is incorrect. See, e.g., DOJ/FBI (continued...)

D. Other Subject-Initiated Dialing and Signaling

In addition to omitting post-cut-through dialed digits, the interim standard also fails to require carriers to provide law enforcement with other important kinds of subject-initiated dialing and signaling information. As explained in the government's petition, an intercept subject (either the subscriber or another person using the subscriber's telephone) may invoke services like three-way calling and call transfer by pressing feature keys or the flash hook. DOJ/FBI Petition ¶ 61. The interim standard fails to provide a call data message when the intercept subject inputs dialing or signaling information within a call in this fashion. For reasons set out in the government's petition, this kind of information constitutes "call-identifying information" under CALEA, and without access to it, law enforcement may find it difficult or impossible to follow the course of the communication or to determine to whom the subject is speaking at any point in the conversation. *Id.* ¶¶ 62-65.

A number of commenters assert that information identifying subject-initiated dialing and signaling activity is not "call-identifying information," and therefore need not be provided, because it does not identify the "origin, direction, destination, or termination" of a communication (47 U.S.C. § 1001(2)). See, e.g., TIA Comments at 47; CDT Comments at 44-45; BellSouth Comments at 10. These arguments all rest in one fashion or another on the industry definition of "call-identifying information" contained in the interim standard. That definition, however, is improperly restrictive and is not faithful to the law enforcement objectives of CALEA. See pp. 30-35 *supra*. Application of that definition to the subject-initiated dialing and signaling activity identified in the government's petition

²⁷(...continued)
Petition, Appendix 2, p. 33; *id.* Appendix 3, p. 16.

would result in a dramatic and wholly unwarranted loss of information with important investigatory and evidentiary value.

Properly interpreted, the statutory definition of "call-identifying information" is amply sufficient to include subject-initiated dialing and signaling activity like the pressing of flash hooks and feature keys to control call forwarding and call transfer. This activity identifies the "direction" and "destination" of the subject's communications. As explained above (see pp. 34-35 supra), "information identifying * * * the direction" of a communication encompasses not only information about the path of the communication through a network, but also information about dialing and signaling activity by the subscriber that directs the communication. When the subject presses a flash hook or feature key to transfer a call or establish a conference call, he is engaged in directing the call, and the carrier is obligated to provide information identifying that "direction." By the same token, information about flash hook and feature key activity is necessary to identify the "destination" of each communication, for without such information, it may be impossible to tell with which party the subject is communicating. As explained in the government's petition, all of this information traditionally has been accessible to law enforcement over the local loop.

CDT asserts that information identifying the persons participating in a call is outside the scope of the pen register statute and that the government therefore is demanding information to which it is not legally entitled. CDT Comments at 44-45. This argument is misconceived in two respects. First, while pen registers and trap-and-trace devices do not directly report the identities of calling and called parties, they provide calling information that law enforcement legitimately may use, in conjunction with other information, to identify persons involved in criminal activity. There is nothing remotely improper, much less unlawful, about such investigatory uses of pen register information. Therefore,

the suggestion that acquiring information about subject-initiated dialing and signaling activity is somehow inimical with the purposes of the pen register statute is baseless.

Second, CDT's argument assumes that information about subject-initiated dialing and signaling activity (and "call-identifying information" more generally) is only relevant and only sought in pen register cases. That is obviously incorrect. Information about subject-initiated dialing and signaling activity is just as important to law enforcement under Title III as it is in pen register cases, if not more so, and a carrier's statutory obligations under Section 103 apply to Title III cases as well as to pen registers. Yet CDT's argument would deprive law enforcement of the capability to acquire this information in all cases, even those involving wiretaps under Title III.²⁸

Taking a different tack, TIA asserts that, for signaling activity that is transmitted from the subject to the network and detected by the switch, the interim standard already provides law enforcement with "all potentially relevant call-identifying information." TIA Comments at 48-49 (emphasis in original). TIA bases this argument on the interim standard's Change message (J-STD-025 § 5.4.4) and certain other messages. Contrary to TIA's claim, however, these messages are not an adequate substitute, practically or legally, for the information sought in the government's petition.

²⁸ As a general matter, none of the assistance capability issues in this proceeding requires the Commission to determine which provision of the federal electronic surveillance statutes authorizes law enforcement to obtain particular information. Section 103(a) of CALEA requires carriers to maintain the capability to provide access to communications and call-identifying information "pursuant to a court order or other lawful authorization." 47 U.S.C. § 1002(a)(1), 1002(a)(2). As long as law enforcement could obtain a "court order or other lawful authorization" to acquire the information in question, it is irrelevant for present purposes whether the information could be acquired pursuant to a pen register order (see 18 U.S.C. § 3123) or whether the government instead would need a Title III intercept order (see *id.* § 2518) or some other form of legal authorization.

The principal shortcoming involves the operation of the Change message. The Change message is generated by changes in call identities. See J-STD-025 § 5.4.4 (Change message triggered when, e.g., "two or more call identities are merged into one call identity" or when "an additional call identity is associated with an existing call"). However, changes in call identities need not -- and for some platforms will not -- correspond to changes in party identities. Manufacturers are free to use a single call identity to cover multiple legs of a call. When this approach is used, subject-initiated signaling activity will not generate a Change message. For example, a subject could press the flash hook to move back and forth between two legs of a call repeatedly without ever generating a Change message. The interim standard does not ensure that the government receives this critical information about the direction and destination of each communication within the call. As a result, TIA is fundamentally mistaken when it asserts (TIA Comments at 49) that the only additional information provided under the government's proposed rule is "the identity of the actual keys pressed" by the subject.

TIA also argues that Section 103 does not obligate a carrier to provide law enforcement with access to "local" subject-initiated signaling activity, such as signaling activity internal to a PBX, that is not detected by the carrier's network. TIA Comments at 50. This argument is based on a misunderstanding of the government's petition and proposed rule. The government is not asking for carriers to provide access to local subject-initiated signaling activity that is not detected by their networks. See DOJ/FBI Petition, Appendix 1, § 64.1708(c)(1). TIA's objections are therefore immaterial.

Finally, BellSouth states that in "some" switch implementations, the detection and collection of off-hook signals and digit dialing occurs in a line module that is separate and distinct from the main

processor of the switch. BellSouth Comments at 11. BellSouth asserts that making this information available to the main processor so that it can be sent to law enforcement "may" require fundamental modifications to the architecture of such switches. Ibid. But the information must be delivered to the main processor at some point if the switch is to carry out the necessary call processing successfully. Moreover, even if BellSouth's claim were true for particular switching platforms, and even if the nature of the needed modifications meant that the information was not "reasonably available" to carriers using those platforms, BellSouth itself does not suggest that all (or even most) platforms would require this kind of redesign. Yet the interim standard excuses all carriers from providing information about subject-initiated dialing and signaling activity, regardless of the particular platform they are using. As explained above, the interim standard is deficient unless it ensures that all carriers who comply with it are delivering the call content and call-identifying information that they are required to provide under Section 103 of CALEA. See pp. 12-13 supra. The fact (if it is a fact) that call-identifying information may not be "reasonably available" to certain carriers does not justify an industry standard that relieves all carriers from the obligation to provide such information.

E. Information on Participants in Multi-Party Calls

The interim standard does not require carriers to provide any message or signaling information indicating that a party has joined a multi-party call, been placed on hold, or dropped from the call. See DOJ/FBI Petition ¶ 73. Without such information, law enforcement would not know who joins or leaves a conference call, whether the subject alternated between legs of the call, or which parties may have heard or said particular communications during the course of the call. Id. ¶ 75. For reasons given in the government's petition, information that identifies party "joins," "drops," and "holds" in multi-party calls constitutes "call-identifying information" under CALEA, and access to such

information has potentially great investigatory and evidentiary value to law enforcement. Id. ¶¶ 75-78.²⁹ The government's proposed rule therefore provides for the delivery of "party join," "party drop," and "party hold" messages.

TIA argues that the interim standard already provides law enforcement with the information that would be provided by the proposed Party Join and Party Drop messages. TIA Comments at 52-53. TIA asserts that the information covered by the Party Join message is already provided by the interim standard's Origination, TerminationAttempt, and Change messages. Ibid. TIA further asserts that the information sought by the Party Drop message is already provided by the Release message. Id. At 52-53. These assertions are incorrect.

The combination of the Origination and Change messages does not serve as an effective proxy for the Party Join message. As already explained in connection with the issue of subject-initiated dialing and signaling activity, the Change message is tied to changes in call identities rather than changes in party identities. See pp. 48-49 supra. As a result, a Change message will not necessarily be generated when a subject joins two parties into a conference call. Indeed, the interim standard itself expressly demonstrates this result. See J-STD-025, Annex D.10.1, Table 28, Step 8 (no Change

²⁹ Several commenters note that, even if a law enforcement agency receives party join and party hold information, it will not necessarily be able to determine or prove that a joined party was actually listening to the conversation. See TIA Comments at 54; AT&T Comments at 10. That is true, but it hardly shows that party join and party drop messages lack evidentiary and investigatory value. In some instances, it may be just as important to law enforcement to know who was not "on the line" at the time of a particular communication as to know who was. Moreover, simply knowing that a particular statement by a subject was directed to one party, rather than to another party, may be significant for the course of an investigation even if law enforcement cannot be completely certain that the party heard the statement. In any event, CALEA does not condition the assistance capability requirements of Section 103 on the telecommunications industry's appraisal of the law enforcement value of particular information; as long information comes within the scope of Section 103, carriers are obligated to provide it to law enforcement.

message generated when subject joins party A and party B). The combination of the TerminationAttempt message and Change message suffers from the same defect.

Turning from party joins to party drops, the Release message is not a substitute for the Party Drop message because the interim standard does not require a carrier to send the Release message when a single call leg or call appearance is released. Instead, it makes the delivery of the Release message for such events discretionary. See J-STD-025 § 5.4.8 ("The Release message may be triggered when a call leg or call appearance is released") (emphasis added). The Release message is mandatory, rather than discretionary, only when an entire call ends. See id. ("The Release message shall be triggered when * * * a completed circuit-mode call is released") (emphasis added). If a particular manufacturer uses a single call identity for all legs of a conference call, the Release message therefore will not be sent until the conference call is completed; the dropping of a single party from the conference call will not generate the message.

With respect to party holds, TIA concedes that the interim standard does not provide any message that corresponds to the proposed Party Hold message. However, TIA argues that information about party holds does not constitute "call-identifying information." TIA Comments at 53-54.³⁰ Other commenters go well beyond TIA's position by arguing that "call-identifying information" does not include any of the information sought by law enforcement regarding party joins, drops, and holds. See, e.g. CDT Comments at 45; USTA Comments at 4; BellSouth Comments at 9.

³⁰ TIA also states that, to the extent that a hold key is not detected by a carrier's network, the hold information is not "reasonably available" to the carrier. TIA Comments at 54. TIA is evidently discussing "local" signaling activity (such as signaling internal to a PBX). As explained above, the government is not asking carriers to provide information about such local signaling activity. See p. 49 supra.

The legal analysis underlying these comments suffers from two closely related shortcomings. First, the statutory definition of "call-identifying information" covers all dialing or signaling information that identifies "the origin, direction, destination, or termination of each communication generated or received by a subscriber * * * ." 47 U.S.C. § 1001(2) (emphasis added). When a subscriber's facilities are supporting a multi-party call, a single call may (and often will) involve more than one "communication." For example, if the subject holds a conversation with one party, then joins another party for a conference call, then drops the first party and continues speaking with the second party, each discussion constitutes a separate "communication." The definition of "call-identifying information" means that the carrier must provide information that identifies the origin, direction, destination, and termination of each of these communications, not simply the call as a whole. (Tellingly, when TIA discusses the Party Hold message (TIA Comments at 53-54), TIA finds it necessary to replace "each communication" with "[a] communication.")

Second, the commenters once again rely on an unduly restrictive reading of "origin, direction, destination, or termination." As explained in the government's petition, each time a subject adds a party to a conference call or a party is dropped or placed on hold, notification of the event identifies the subject's direction of each communication making up the conference call and the destination of each communication. See DOJ/FBI Petition ¶ 78. As a result, party join, party drop, and party holding information constitutes "information that identifies the * * * direction [and] destination * * * of each communication" involved in the call.

In the government's rulemaking petition, we noted that law enforcement has not historically had the technical capability to obtain information showing that joined parties have been placed on hold or dropped from multi-party calls, because such information resides in the switch and cannot be

accessed from the local loop. See DOJ/FBI Petition ¶ 77. Several commenters suggest that the lack of traditional access to this information places it outside the bounds of Section 103(a)(2). See, e.g., USTA Comments at 4; PrimeCo Comments at 14. As already discussed, however, traditional capabilities are not dispositive regarding the scope of CALEA. See pp. 10-11 supra. Here, the statutory language is sufficiently clear, and the investigatory and evidentiary weight of the information sufficiently integral to the law enforcement goals underlying CALEA, to support the conclusion that carriers are obligated to provide access to the information.

BellSouth and USTA assert that delivery of party join, party drop, and party hold messages to law enforcement at the subscriber's switch may be technically difficult when a conference call is handled by a conferencing bridge element that is remote from the switch. BellSouth Comments at 9-10; USTA Comments at 5.³¹ However, in the case of conventional three-way or six-way conference call services, the conference call feature is supported in the switch. And for some platforms, even the kind of conferencing bridge service described by BellSouth is available within the switch. At the very most, therefore, the comments indicate that party join, party drop, and party hold messages may not be "reasonably available" in all circumstances. The interim standard, however, does not require carriers to provide these messages in any circumstances. For that reason, the interim standard is plainly deficient.

³¹ These comments assume that the intercept access point (IAP) is necessarily at the switch. There is no basis in CALEA for that restrictive assumption, and the interim standard itself does not make such an assumption. For example, the interim standard requires Home Location Registers (HLRs), which are not necessarily part of the switch, to report serving system messages and feature information. See J-STD-025 § 3, p. 8 (definition of IAP); id. Annex A, Figure 12.

F. Notification of Network-Generated In-Band and Out-of-Band Signaling

When a call attempt is made to or from a subscriber's equipment, facilities, or services, the carrier's network generates in-band or out-of-band signaling that identifies call progress. These signals may be presented to the subject as audible tones, visual indicators, or alphanumeric display information. For outgoing call attempts, these signals indicate (for example) whether the call attempt ended with a busy signal, ringing, or before the network could complete the call. For incoming call attempts, these signals indicate (for example) whether the subject's telephone received a call waiting tone or was alerted to the redirection of a call to voice mail by a "stutter" tone or a message-waiting light. Collectively, these signals show how the network treated a call attempt: whether or not it was completed, how the call may have been redirected or modified, and how the call ended.

The interim standard does not require carriers to provide law enforcement with notification of network-generated call progress signals. For reasons set forth in the government's petition, carriers are obligated to provide access to this information under Section 103(a)(2) of CALEA, and the omission of the information renders the interim standard deficient. See DOJ/FBI Petition ¶¶ 80-81.

1. A number of commenters assert that network-generated call progress signals are not call-identifying information or, more narrowly, that particular signals (such as busy tones and call waiting indicators) are not. See, e.g., TIA Comments at 56-57, CDT Comments at 45-46; BellSouth Comments at 11; Nextel Comments at 11; SBC Comments at 12; AT&T Comments at 11-12. As explained in our petition, however, all of the signals at issue here identify the "direction," "destination," and/or "termination" of a communication. DOJ/FBI Petition ¶ 81. A call attempt may "terminate" with ringing (without an answer), with a busy tone, or with a trunk busy signal; signaling

such as this conveys information on call termination and therefore constitutes call-identifying information. Similarly, a network-generated call-waiting tone or a "stutter" tone identifies the "direction" or "destination" of the call and is therefore likewise call-identifying information.

Several commenters assert that the definition of "call-identifying information" excludes information identifying how a call attempt terminates. See, e.g., AT&T Comments at 12. But nothing in the language of the statutory definition suggests such a limitation. A call attempt that ends with a busy signal and one that ends with ringing have different "terminations"; only by learning the network-generated signal can law enforcement identify the specific termination of the call attempt. Here, as elsewhere, the commenters are relying on an unduly restrictive reading of "call-identifying information," one that would exclude significant information to which law enforcement traditionally has had access over the local loop.³²

TIA and several other commenters state that when signaling information is generated by a remote network switch, such as a busy signal generated in an outgoing long-distance call, the signaling information is not "reasonably available" to the subscriber's local carrier, and therefore is not within the local carrier's assistance capability obligations under Section 103(a)(2), because the local carrier's switch is not equipped to detect busy signals and other tones generated by remote switches. See TIA Comments at 58-59; USTA Comments at 5; BellSouth Comments at 12; SBC Comments at 12. These comments reflect a misunderstanding of the scope of the government's

³² The government does not contend, as TIA suggests (TIA Comments at 59-60), that network-generated signals like ringing constitute call-identifying information because they can be used by criminals to convey pre-arranged messages. Ringing and other tones can indeed be used for such purposes, and that is one reason why it is important for law enforcement to have access to them, but they are call-identifying information for a different reason -- because they identify the termination of the call.

petition. The government is not asking a carrier to provide notification of in-band and out-of-band signaling generated outside the carrier's own network. The government's proposed rule is limited to in-band and out-of-band signaling "from the subscriber's service" -- that is, signaling generated by the carrier providing the subscriber's service, not signaling generated by another carrier. See DOJ/FBI Petition, Appendix 1 (§ 64.1708(d)); see also id. § 64.1708(d)(1) ("accessing system"). As a result, when (for example) a subscriber places a long-distance call and receives a busy signal generated by the called party's carrier, the subscriber's carrier would not be required to deliver a notification message of the busy signal to law enforcement.

2. In addition to arguing that network-generated call progress signals are not "call-identifying information," TIA argues that the interim standard already provides much of the information sought by the government. See TIA Comments at 56-61. However, TIA considerably overstates the comprehensiveness and effectiveness of the interim standard.

TIA suggests that "most" audible signaling tones (such as busy signals) are available to law enforcement over call content channels, thereby eliminating the need for delivery of a notification message regarding audible tones. TIA Comments at 57-58; see also USTA Comments at 5-6; PrimeCo Comments at 16-17. However, the interim standard requires delivery of call content to law enforcement only between call completion (answer) and call release. See J-STD-025 § 4.5.1 There is no requirement that the carrier deliver call content on incoming calls before they are answered. Instead, the interim standard provides only that "[c]all content may be delivered before answer and may include call progress tones or announcements." Ibid. (emphasis added).

In addition, even when call content is being delivered to law enforcement, the call content channel running from the switch to law enforcement may not reflect the call progress tones being

delivered from the switch to the subscriber's terminal. For example, wireless and ISDN networks send out-of-band "alert" messages that tell a subscriber's terminal to ring or generate some other signal. Law enforcement cannot detect the resulting tones by monitoring the call content channel, because the tones are not being generated at the switch.³³

TIA also suggests that the interim standard's existing data messages convey all of the call-identifying information that is conveyed by audible tones such as busy signals and stutter dial tones. See TIA Comments at 56-57. However, the data messages cited by TIA provide no information about how the call terminated. Nor do they disclose what signals, if any, were presented to the subject -- for example, whether the subject received notification of an incoming call through a call waiting tone. TIA's argument in this regard depends entirely on its restrictive reading of the meaning of "call-identifying information."

With respect to alphanumeric display information, TIA states that the TerminationAttempt message provides the telephone number of the calling party. TIA Comments at 60. But just as the TerminationAttempt message is an inadequate substitute for audible tones, so too is it an inadequate substitute for alphanumeric display information. For example, an alphanumeric display may notify the subject that a call has been redirected to the subscriber's voice mail box. Neither the TerminationAttempt message nor the Redirection message would disclose that a message had been left for the subject. And if a calling party can access the subject's voice mail box directly, rather than by being redirected from the subject's phone number, law enforcement will have no idea that the call

³³ When audible call progress tones are available over a call content channel, the government does not contend that a carrier must provide notification of the tones over a call data channel in order to comply with Section 103. Nevertheless, for reasons set forth above (see pp. 44-45 supra) and in the government's petition (DOJ/FBI Petition ¶¶ 83-85), the Commission properly may include delivery over a CDC in standards adopted by the Commission.

has even been made unless it receives notification of the alphanumeric information alerting the subject to the call.

G. Timely Delivery of Call-Identifying Information

1. Section 103(a)(2) of CALEA obligates carriers to make call-identifying information available to law enforcement "before, during, or immediately after the transmission of a wire or electronic communication" and "in a manner that allows it to be associated with the communication to which it pertains." 47 U.S.C. § 1002(a)(2). Law enforcement's ability promptly to obtain call-identifying information and correlate it with the communication to which it pertains can be crucial, directly affecting law enforcement's ability to respond in emergency and life-threatening cases, as well as enabling law enforcement to "minimize" the interception of non-criminal communications to protect privacy. Yet, as explained in the government's petition, the interim standard imposes no requirement with regard to when call-identifying information must be delivered to law enforcement. This omission renders the interim standard deficient.

TIA asserts that law enforcement's claimed need for timely delivery of call-identifying information rests solely on "colorful" but "imaginary" examples that the government has "conjure[d] up." TIA Comments at 63-64. This assertion betrays a striking insensitivity to, and ignorance of, the actual state of affairs in the realm of electronic surveillance. Although the Commission undoubtedly can appreciate the real-world consequences of law enforcement's lack of timely access to call-identifying information without being presented with a litany of examples, TIA's comments make an illustrative response necessary.

At approximately 11:30 p.m. on January 25, 1996, a 35 year-old woman was abducted near her home in Queens, New York. Her kidnapers took her to a basement and telephoned her husband

in China and her relatives in New York City, demanding \$38,880 in ransom. Her husband heard her screaming in the background as the kidnapers made their demand. After being alerted to the situation, the New York City Police Department (NYPD) obtained court authorization and installed a wiretap and a trap and trace device on the victim's New York relatives' telephone -- a standard strategy in kidnaping cases. However, the carrier was unable to trace the kidnapers' calls quickly enough through its switches and trunk lines to identify the number from which the calls were being made. For days, the NYPD was able to listen to the kidnapers' threatening calls to the victim's relatives but could not determine where the woman was being held. As the kidnapers' deadline for payment neared, their calls became progressively more menacing. When the NYPD finally was able to determine the kidnapers' number, go to the location where the woman was being held, and rescue her, she had been held for thirteen days. Her kidnapers had raped and beaten her daily during this period. See Declaration of Detective John Ross (attached); Dan Morrison, 13 Days in Hell: City, China cops rescue kidnaping, rape victim, NEWSDAY, Feb. 9, 1996, at A3.

In a related vein, AT&T states that it is "patently absurd" to suggest that carriers would delay the delivery of call-identifying information to law enforcement for hours or days. AT&T Comments at 14 n.48. We wish this were so. Turning again to the experience of the NYPD, one New York City carrier's standard time frame for delivering call-identifying information to law enforcement is two days after the call has occurred. The NYPD has heard subjects advise each other to switch to digital technology in order to foil interceptions, and has repeatedly been frustrated in its efforts to collect the pertinent information in time to make effective use of it. See Declaration of Detective John Ross (attached). These real-life examples should make it abundantly clear that law enforcement's need for timely delivery of call-identifying information is anything but "imaginary."

2. Many of the comments are directed not at the underlying need for timely delivery of call-identifying information, but rather at the details of the specific timing requirements in the government's proposed rule. These comments fail to come to terms with the basic point of the government's petition -- namely, that the interim standard is deficient because it lacks any requirements for timely delivery. The Commission's first order of business should be to ask whether an industry standard that places no requirements at all on carriers regarding how quickly call-identifying information must be delivered to law enforcement is adequate to ensure that carriers meet their statutory obligations under Section 103(a)(2). In our view, that question admits of only one answer.

To the extent that the commenters do address the underlying deficiency issue, their arguments are misconceived. The commenters argue that the interim standard is not deficient because Section 103 does not itself impose any "explicit maximum delivery time." TIA Comments at 66; see also CTIA Comments at 17; AirTouch Comments at 20; AT&T Comments at 14. But all of the assistance capability requirements of Section 103 are framed in general, rather than specific, terms; the whole point of the standard-setting process is to give specific content to the general provisions of Section 103 by identifying more precisely what steps are required for a carrier to meet its underlying assistance capability obligations. Omissions from the interim standard therefore can hardly be defended on the theory that there are no correspondingly precise terms in Section 103 itself. A fortiori, the lack of a specific timing requirement in Section 103 cannot excuse the absence of any timing requirement in the interim standard.

Equally misguided is the argument that any specification of a time frame for delivery of call-identifying information would be "arbitrary." USTA Comments at 6; BellSouth Comments at 13;

SBC Comments at 12. A specified maximum time for the delivery of call-identifying information would be no more "arbitrary" than any other specific item already included in the interim standard.

The assertion that the government's proposal represents an attempt at "dictating" a specific system design, in violation of Section 103(b)(1) of CALEA, is mistaken. See SBC Comments at 12. Simply requiring that call-identifying information be delivered within a particular time frame hardly constitutes "requir[ing] any specific design" of a carrier's equipment or system configuration (47 U.S.C. § 1002(b)(1)), any more than requiring the delivery of a specified data message does so. Carriers choosing to satisfy their obligations by means of the Commission's standards will remain free to provide this capability using any equipment or design they prefer. Moreover, as noted above, no carrier is mandated to comply with the specific provisions of the Commission's standards if it can meet its assistance capability obligations by other means.

The assertion that any maximum time frame for the delivery of call-identifying information would ignore the diversity of carriers and compliance solutions in the industry, or the possibility of congestion on the network (see, e.g., AirTouch Comments at 21; PrimeCo Comments at 18), must be rejected. The specific time frame recommended in the government's proposed rule -- three seconds after the associated call event -- was deliberately selected with a view towards making compliance feasible for diverse carriers utilizing various solutions, operating in an environment which may at times face network congestion. In fact, the vast majority of carriers routinely and normally deliver call-identifying information as necessary to perform call setup and takedown in well under three seconds, commonly in a matter of microseconds. The fact that the suggested

standard only requires 99% reliability with regard to timely delivery represents a further attempt to take these factors into account.³⁴

Finally, TIA argues that requiring delivery of call-identifying information within three seconds of the associated event conflicts with the language in Section 103(a)(2) allowing delivery of call-identifying information "immediately after" the transmission of a wire or electronic communication. TIA Comments at 65. In TIA's view, this language shows that a carrier need not provide call-identifying information until immediately after the completion of "the call," and thus if a call lasts for several hours (as many types of calls involving criminal activity -- especially illegal gambling -- typically do), call-identifying information pertaining to events that took place at the beginning of the call or during the course of the call may be delivered en masse hours later, when the call is completed. See ibid. ("Congress certainly envisioned telephone calls lasting longer than three seconds").

This argument cannot be squared with the actual terms of Section 103(a)(2). First, Section 103(a)(2) does not tie a carrier's timing obligations to "the call," as TIA's argument suggests. Instead, the carrier must deliver call-identifying information "before, during, or immediately after the transmission" of the "wire or electronic communication" to which the call-identifying information "pertains." 47 U.S.C. § 1002(a)(2)(A) (emphasis added). A single call may encompass any number of "communications." See 18 U.S.C. § 2510(1) (defining "wire communication"); id.

³⁴ As Ameritech notes, an industry standards committee is currently considering a proposal for delivering call-identifying information within "a maximum of three (3) seconds at least 98% of the time." Ameritech Comments at 8. This casts considerable doubt on other commenters' objections to the feasibility of delivering call-identifying information within a maximum of three seconds at least 99% of the time.

§ 2510(12) (defining "electronic communication"); 47 U.S.C. § 1001(1) (incorporating definitions in 18 U.S.C. § 2510).

Second, Section 103(a)(2) requires delivery of call-identifying information before, during, or immediately after "the transmission of" each communication. 47 U.S.C. § 1002(a)(2) (emphasis added). TIA's argument effectively replaces "transmission" with "completion," so that the delivery obligation does not arise until the call is over. The transmission of a communication is a continuous, ongoing process, not something that occurs only when the communication ends, and the timely delivery obligations of Section 103(a)(2) are correspondingly ongoing.

Finally, TIA's argument ignores Section 103(a)(2)(B), which requires call-identifying information to be delivered "in a manner that allows it to be associated with the communication to which it pertains." 47 U.S.C. § 1002(a)(2)(B). When a call continues for lengthy period, law enforcement cannot associate the call-identifying information with particular communications in a meaningful way if delivery of the call-identifying information is postponed -- as the interim standard permits it to be -- until hours later. As explained in the government's petition, for example, a communication that occurs at the beginning of an hour-long call might involve a direction to carry out a killing immediately -- if law enforcement cannot obtain the call-identifying information pertaining to this utterance until an hour or more later, it may well be unable to prevent the murder. Requiring the prompt delivery of the pertinent call-identifying information will ensure that law enforcement can "associate" the information with the communication in a meaningful and effective way.

3. In order to ensure that law enforcement can correlate individual "wire or electronic communications" with their respective call-identifying information, the government's proposed rule

also provides for an accuracy rate of 100 milliseconds for the time stamps that show when particular triggering events occurred. The few objections raised against this proposal cast no doubt on our observation that the interim standard suffers from a deficiency in this respect, nor do they identify any valid reason for the Commission to reject our proposed solution.

TIA asserts that the accuracy rate of 100 milliseconds is not "reasonably available" because an event can occur in a part of the network far distant from the place at which the time-stamp is affixed. See TIA Comments at 67. This comment appears to misunderstand our recommendation. We seek to be assured of the accuracy of the recording only of events that occur when a network element acts upon a subscriber's input in the ways specified in our proposed rule. See Proposed Rule § 64.1708(d). We do not, for example, request a time-stamp accurate to within 100 milliseconds indicating when a subscriber has pressed a key on a wireless telephone.

TIA also maintains that there is no deficiency in the interim standard because that standard provides for a time-stamp to be affixed when the triggering event is detected at the "intercept access point" (i.e., the point in the network used to access call-identifying information for the purposes of an intercept). See TIA Comments at 66-67. TIA does not explain how a standard can be thought to require an adequate level of accuracy when it in fact requires no particular level of accuracy.

Finally, BellSouth objects that it would be expensive to synchronize the carriers' switches to Universal Coordinated Time. See BellSouth Comments at 12-13. But we are not asking carriers to create such synchronization, and in fact the very purpose of our recommendation regarding the accuracy of the time-stamp is to make synchronization unnecessary. If law enforcement can be confident of the accuracy of the time-stamp to within 100 milliseconds, it can ascertain the difference between the time kept by the clock affixing the time-stamp on the call data channel, and

the time kept by the clock to which events on the call content channel are referenced, by comparing the time derived from each of these methods for the initiation of a call. Other events occurring during the call can then be correlated using this fixed time differential. If the accuracy of the time-stamp is not assured, however, it will be impossible for law enforcement to determine whether the differential should be ascribed to the difference between the two clocks' settings, or to delays between the event and the affixing of the time-stamp.

H. Automated Delivery of Surveillance Status Information

1. Section 103(a) of CALEA provides that a telecommunications carrier "shall ensure" that its equipment, facilities, and services are capable of isolating and delivering communications and call-identifying information to law enforcement. Section 103 thus places an affirmative obligation on the carrier to verify that its equipment is operational and that law enforcement has access to all communications and call-identifying information within the scope of the authorized surveillance. However, the interim standard does not contain any provisions that give effect to this affirmative statutory obligation.

To cure this deficiency, the government's petition proposes that the Commission add three elements to the interim standard: (i) a continuity tone, which would enable law enforcement to confirm that "all" (and not only a subset) of the communications subject to surveillance authorization and carried by a carrier to or from its equipment, facilities, or services were intercepted, CALEA § 103(a); (ii) a surveillance status message, which would record the activation, updating, and deactivation of any surveillance, as well as periodically signaling law enforcement that the surveillance is functional; and (iii) a feature status message, which would record any changes in a subscriber's call features and services. See DOJ/FBI Petition at 52-57. The

commenters have failed to refute either our assertion that the absence of any mechanism for providing surveillance status information represents a deficiency in the interim standard, or that our suggested methods for curing this deficiency should be included in the Commission's standards.

A few comments attempt to counter our fundamental assertion that the absence of any requirement for the delivery of surveillance status information represents a deficiency in the interim standard, but these comments misunderstand the nature of the relationship between the interim standard and Section 103. As explained above, Section 103 does not require any specific method of complying with its general assistance capability obligations. Thus, it is quite beside the point to argue that the specific requirements that we have recommended for inclusion in the Commission's rule are not expressly required by Section 103. Neither is it the case, as TIA suggests, that we are trying to insert "second-order obligations" into Section 103 (TIA Comments at 68); we are relying instead on a carrier's primary obligation under Section 103 to "ensure" that its equipment is capable of providing access to the information specified by CALEA. Because the interim standard fails to address this issue, these objections must be rejected.

2. As explained in the government's petition, law enforcement's ability to make effective use of information collected in an interception often depends on its ability to verify that all of the communications subject to surveillance authorization and carried by a carrier to or from its equipment, facilities, or services were intercepted during the relevant period. If law enforcement cannot verify that this is the case, a defendant could claim that non-intercepted communications undermined the significance placed on intercepted communications by law enforcement, for example by ascribing innocuous meanings to expressions that law enforcement describes as code words for illegal activity. The government's proposed rule therefore provides for a "continuity tone"

that will verify that the call content channels between the carrier and law enforcement are operational.

One commenter states that it "supports the use of a continuity tone if its use is limited to instances where dedicated content delivery channels from the switch to LEA locations are involved." BellSouth Comments at 15. This is precisely what the government is recommending. BellSouth's readiness to provide the precise capability that the government is requesting casts serious doubt on the representations by other commenters that providing this capability would be prohibitively complex or expensive.

A few commenters assert that this proposal represents an impermissible attempt by law enforcement to "dictate" the manner in which the industry complies with CALEA. SBC Comments at 13; AT&T Comments at 13; AirTouch Comments at 24. This assertion has nothing to do with the essential issue of whether the lack of such a provision in the interim standard constitutes a deficiency, and as we have explained above, it fundamentally misunderstands the nature of this proceeding. Furthermore, the government's proposal would not require any carrier to implement any particular design or equipment, because even carriers choosing to follow the Commission's standards may provide the continuity tone by means of any equipment they prefer.

One commenter argues that a continuity tone has "nothing to do with call identifying information or the content of communications." SBC Comments at 13. But the government does not contend that a continuity tone is itself call-identifying information or call content; instead, it is a means of satisfying the carrier's obligation to "ensure" the effective delivery of such information. The information provided by a continuity tone is absolutely essential to law enforcement's ability to make effective use of electronic surveillance. Without such a means of attesting to the continuous

functioning of an intercept, law enforcement's ability to use information gathered through electronic surveillance to build cases against criminals is severely undermined. This is why law enforcement has always created its own continuity tones when conducting pre-digital wiretaps -- because this verification capability in fact has everything to do with the effective use of legally-authorized surveillance.

PrimeCo warns that a carrier "cannot reasonably be expected to monitor whether the delivery channels [leased by law enforcement from a local exchange carrier] have failed." PrimeCo Comments at 20; see also AirTouch Comments at 25. The government certainly does not seek to hold a carrier responsible for the maintenance of a continuity tone over lines that it neither controls nor has contracted to utilize, and a carrier would not lose the protection of the safe harbor because the continuity tone was interrupted due to a flaw in a system for which they are not responsible. However, there is no logical reason to excuse a carrier from providing a reliable tone simply because it has contracted for the use of lines, rather than using only its own lines.

PrimeCo also states that circuits already have "special tone or idle pattern[s]," and suggests that law enforcement simply make use of these. PrimeCo Comments at 20. The government has no objection to the use of existing tones or idle patterns, and would accept the use of any already-existing tones or patterns that could match the functionality of the continuity tone that we have described. To reiterate, our principal purpose is neither to seek to require particular methods of complying with Section 103, nor even to require particular methods of curing the deficiencies that we have identified in the interim standard. If carriers can provide the Commission with other, equally effective methods of curing these deficiencies, the government has no objection to the use of such methods.

Some commenters object that providing law enforcement with a continuity tone would require expensive modifications of existing switches. TIA Comments at 69; AirTouch Comments at 24. To the extent that these commenters are simply relying on cost considerations, their objections may be relevant to relief under Section 109(b) but are not relevant to the scope of a carrier's underlying obligations under Section 103. See p. 35 supra. In any event, providing a continuity tone or its equivalent should require no major modifications of existing systems, because carriers already use digital bit patterns for maintenance oversight on their trunk lines. The government has no objection to carriers using these same features to provide the functional equivalent of a continuity tone. The Commission is free to consider any alternative means of curing this deficiency that would be more acceptable to the industry than the continuity tone while providing the same functionality.

3. The interim standard also fails to give law enforcement a means of determining whether interception software is accessing the correct equipment, service, or facility. The government's petition and proposed rule seek to cure this deficiency by including a provision for the automated delivery of surveillance status messages, which would indicate that the interception is working correctly and is accessing the correct subscriber's service. This provision would implement the requirement in Section 103 that a carrier "shall ensure" that its facilities are capable of delivering the surveillance information that law enforcement has requested through a court-authorized interception, as well as ensuring that law enforcement can make effective use of this information.

US West argues that Section 103's "shall ensure" language merely "impl[ies] a duty to provide reliable electronic surveillance service." US West Comments at 23. US West does not explain how a carrier that leaves law enforcement in the dark as to whether its intercepts are

properly connected, functioning, capable of collecting all of the information crucial to an investigation, and attached to the proper individual's lines could nevertheless be thought to provide "reliable electronic surveillance service." Nor does it attempt to counter our observation that, without the surveillance status information that we have described, law enforcement will be unable to make use of the surveillance information it collects. The "shall ensure" language in Section 103 reinforces a fundamental fact that neither this nor any other commenter can undermine: law enforcement must be able to monitor the status of its surveillances in order to make effective use of legally-authorized interceptions.

PrimeCo argues that a more reasonable method for law enforcement to verify whether a wiretap is operational would be to "perform a periodic trap and trace test of the target's phone number to verify that it is working." PrimeCo Comments at 20. PrimeCo apparently means to suggest that law enforcement should place periodic calls to the subject's phone, each time perhaps pretending that it had dialed a wrong number, and evaluate the soundness of the interception during these calls. Aside from being absurdly contrary to the common-sense notion that surveillance should be as unobtrusive as possible, this "solution" would violate the specific mandate of Section 103(a)(4) of CALEA, which requires that interceptions be conducted "unobtrusively" and "in a manner that protects * * * information regarding the government's interception of communications and access to call-identifying information."

TIA asserts that providing a surveillance status message would be unduly burdensome and costly. See TIA Comments at 70. This comment effectively rests on the premise that carriers have no mechanism in place for determining whether any or all of the circuits that make up their networks are functioning. Of course, carriers have such mechanisms in place, and without them they would

be unable to conduct their business. Many have worked extensively to develop these infrastructures in cooperation with Subcommittee T1M1 and the TR45.7, in an effort known as the Telecommunications Management Network.

The optional "connection test message" of the interim standard is not, as one commenter claims (see USTA Comments at 6), sufficient to meet law enforcement's need for surveillance status information. The first reason for its inadequacy is that it is optional, and thus carriers are not required to provide it at all. Second, unlike the government's proposal, the connection test message comes with no "triggers," or meaningful junctures at which the relevant information would be delivered. Finally, the connection test message contains no assurance to law enforcement that its intercepts are properly provisioned in the network, meaning that it is incapable -- for example -- of alerting law enforcement to the fact that an intercept is attached to the wrong subscriber's line.

BellSouth notes that various distribution architectures will require diverse solutions for the provision of surveillance status information. BellSouth observes that in the cellular context, for example, surveillances are necessarily distributed (because a subject may move from one cellular transmitter and its respective switch to another during a single communication). See BellSouth Comments at 13. We agree. Once again, we stress that our main concern is that the deficiencies we have identified in the interim standard be corrected. We have repeatedly noted that our specific suggestions for correcting these deficiencies might not represent the only available means for doing so. In this context, we are open to any solution that proves convenient for carriers dealing with various distribution architectures while preserving the functionality required by Section 103. If, for example, a cellular carrier finds it more convenient to aggregate information from dispersed

locations into a single surveillance status message, we could support that solution if it were to promise a functionality sufficient to satisfy Section 103's requirements.

AT&T suggests that "human intervention" is adequate to cure the deficiency identified by the government. See AT&T Comments at 13. This suggestion is entirely at odds with the present-day reality of "human intervention." Law enforcement has attempted to obtain this information by calling carriers and asking them to send technicians to check on intercepts, but has found this process to be extremely ineffective. Faced with rapidly-unfolding events in an investigation, law enforcement often finds itself desperately in need of assurances with regard to the status of a wiretap at odd hours, when none of the carrier's technicians is available to conduct the necessary checks. Hiring the number of technicians necessary to meet law enforcement's needs, and paying them to be available around the clock (as automated status reporting systems are), would be far from a cost-effective solution, from the perspective either of the carriers or of law enforcement.

4. Finally, the interim standard does not require carriers to "ensure" that their equipment is capable of intercepting all information pertinent to a legally-authorized interception by enabling law enforcement to know when and how the calling features and services available to a subscriber have changed. As a means of curing this deficiency, the government's petition and proposed rule include a provision for the automated delivery of a feature status message that would notify law enforcement of such changes.

TIA states that it is unclear whether we are suggesting that law enforcement be informed whenever a subscriber requests a change in service, or rather only when a change in service becomes effective for a subscriber, and argues that the former requirement would be burdensome to implement. See TIA Comments at 70-71. We propose only the latter requirement, and thus TIA's

arguments regarding the feasibility of the former are irrelevant. By mounting no challenge to the latter requirement -- which represents our actual proposal -- TIA appears to concede that it would not impose any unreasonable burdens. See id.

A few commenters claim that our proposal would not serve its intended purpose because subscribers can make use of special features on a per-call basis, rather than solely by requesting more long-term changes in their service profiles. See BellSouth Comments at 14; USTA Comments at 6; SBC Comments at 14. But the availability of per-call features is simply irrelevant to our proposal. We have suggested only that law enforcement be alerted to the assignment or removal of features that can affect call content or call-identifying information from a customer's line, and have not sought to be notified of a subscriber's use of per-call features. As a practical matter, law enforcement will know in advance what per-call features a particular carrier makes available to its subscribers, and will have collected enough information to predict the subject's likely use of such features, before initiating an intercept, and will be able to order the appropriate number of call content and call data channels based on this information.

Some commenters seek to base objections on the development of Advanced Intelligent Network services. See BellSouth Comments at 14; USTA Comments at 6. Nothing that we have proposed has any bearing upon a carrier's ability to develop Advanced Intelligent Network systems, and none of our proposals is incompatible with these systems. If they were, we would welcome the suggestion of alternative means of curing this deficiency that would be compatible with these new systems. Once again, however, the commenters have declined either to challenge our fundamental observation that there are deficiencies in the interim standard, or to suggest alternatives to our proposed means of curing these deficiencies.

Some commenters again argue that the government's proposal seeks the delivery of information that has nothing to do with the origin or destination of a call, and thus is not call-identifying information. See BellSouth Comments at 13-14; PrimeCo Comments at 20-21; SBC Comments at 13. These commenters fail to recognize the statutory obligation to "ensure" that carriers' systems are capable of providing law enforcement with "all wire and electronic communications" essential to an authorized interception (47 U.S.C. § 1002(a)(1)). They do not attempt to, nor could they, undermine our observation that information regarding changes in a subscriber's service profile are absolutely essential to law enforcement's ability to conduct effective electronic surveillance.

One commenter refers to various complications that might arise when changes in features or services occur outside of a carrier's network, and thus are not reflected in the carrier's records. See PrimeCo Comments at 21. This is a red herring, for the government is not suggesting that any carrier report to law enforcement regarding service changes implemented outside of its network. See DOJ/FBI Petition, Appendix 1 (§ 64.1708(g)) (specifying "network-provided" features). Nor have we suggested that feature status reporting should include obscure and inconsequential features that could not affect law enforcement's ability to conduct effective surveillance. See *id.* (specifying "features that would affect the delivery to law enforcement of call content or call-identifying information"); *id.* at (g)(2) (enumerating specific categories of features).

Ignoring the fundamental changes in telecommunications services that led Congress to enact CALEA itself, a few commenters declare that law enforcement should be satisfied with making person-to-person requests for feature status information. See AT&T Comments at 13; CDT Comments at 20; CTIA Comments at 17; U S West Comments at 24. This method of obtaining this

information is infeasible in the current environment. Law enforcement officers in one city urgently needing feature status information can no longer simply identify the appropriate carrier employee in the carrier's local office, serve that person with a subpoena, and quickly obtain the necessary information. The employees who could have serviced such requests in the old environment do not exist today; they have been replaced by computerized switching systems that may be located in an entirely different city from the law enforcement officer needing the information. Given the current structure of telecommunications service, automated messaging clearly is the most practicable and convenient method of meeting this need, for law enforcement and for telecommunications carriers.

I. Standardization of delivery interfaces

As explained in the government's petition, the implementation of CALEA's assistance capability requirements could be jeopardized by the development of numerous incompatible interface protocols, for each of which law enforcement would have to develop individualized interface mechanisms in order to make use of surveillance information. The practical difficulties of managing interfaces with countless different protocols would cause law enforcement to be effectively denied access to information both legally authorized for collection and actually collected by carriers. To cure this deficiency, the government's petition and proposed rule seek a limit on the total number of interfaces used.³⁵ The petition emphasizes that the government is not trying to

³⁵ Contrary to the suggestion of AirTouch (see AirTouch Comments at 25), the position taken in the government's petition and proposed rule regarding limits on the number of interfaces is precisely the same position taken by the Department of Justice in its February 3, 1998, letter to industry. See DOJ/FBI Petition, Appendix 5, at 3 ("although a single delivery interface is not mandated by CALEA * * * [r]ecent productive discussions with industry have resulted in what DOJ believes is an acceptable compromise, whereby the industry would commit to a limited number of no more than five delivery interfaces") (emphases added). AT&T is incorrect when it claims that the government has subsequently characterized the request for a five-interface limit as "unnecessary and (continued...)

prescribe particular interfaces to be included in the Commission's rule, that CALEA itself does not require the adoption of any particular interface, and that the government seeks only to ensure that law enforcement will not be presented with an unmanageable multiplicity of incompatible protocols. This proposal clearly does not contemplate any onerous restructuring or cutting back of existing protocols since, as TIA concedes, the number of protocols generally used by carriers is already quite limited. See TIA Comments at 74; cf. BellSouth Comments at 16 (alleging that the proposal would require widespread modification of existing equipment).

Only a few comments even attempt to cast doubt upon the reasonableness of this proposal. One commenter claims that the interim standard's rules governing the format of acceptable physical interfaces adequately meets law enforcement's concerns. See TIA Comments at 73. But the interim standard in no way limits the number of different physical interfaces law enforcement will have to manage, and thus does nothing to meet the concern underlying this proposal.

Two commenters make the irrelevant assertion that CALEA requires no specific interface, and that industry should be left the task of choosing particular interfaces. See TIA Comments at 72; SBC Comments at 14. As we have stressed, our proposal in no way suggests that law enforcement or the Commission mandate the adoption of any particular physical interfaces by any carrier.

Finally, TIA asks what is to be done when the evolution of telecommunications technology leads to the introduction of new interfaces. See TIA Comments at 74. We note that law enforcement did not invent the problem of multiple incompatible interfaces, and that it has always

³⁵(...continued)

not required." AT&T Comments at 15-16. That claim rests on a misrepresentation of the government's statements to the ESS ad hoc group. See Letter from H. Michael Warren, Senior Project Manager/Chief, CALEA Implementation Section, FBI, to Peter Musgrove, Chair, TIA TR45.2 ESS Ad Hoc Group (June 1, 1998), p. 2 (attached).

been an issue that the industry itself has had to deal with in designing its products, for example by creating industry standards and updating these standards periodically to reflect changes in the relevant technologies. Law enforcement has no objection to the same approach being taken in this context, through the mechanism made available in CALEA. Should the industry decide that a new interface is desirable, the Commission may readily provide for the use of that interface.

III. Other Assistance Capability Issues

A. Location Information

In its rulemaking petition, CDT has objected to provisions of the interim standard that require carriers, in certain circumstances, to provide law enforcement agencies with "location" information at the beginning and end of communications to and from mobile terminals. In its latest comments, CDT renews these objections. See CDT Comments at 29-34.

In our comments filed on May 20, we addressed this issue and explained why CDT's objections are unfounded. See DOJ/FBI Comments at 16-21. As we noted, the language in Section 103(a)(2) of CALEA concerning location information does not demonstrate that location information is not "call-identifying information"; to the contrary, it reflects precisely the opposite assumption. The language on which CDT relies is intended only to ensure that location information is not provided on the basis of a pen register order, and the provisions of the interim standard are fully consistent with that requirement. In practical terms, moreover, the interim standard does not require carriers to provide information that would permit law enforcement agencies to identify the specific physical location of an intercept subject. CDT's current comments require little further discussion; only two additional comments are in order.

First, contrary to CDT's suggestion (CDT Petition at 32-33), the government is not trying to turn Section 103(a)(2)'s express exception regarding location information in pen register cases into a "mandate" in non-pen register cases. Rather, we are simply saying that the exception is just that -- an exception -- and that outside the context of pen register cases, the general definition of "call-identifying information" applies. It is CDT that is trying to turn Section 103(a)(2)'s limited proviso regarding location information in pen register cases into an omnibus exclusion of location information from the scope of CALEA, an exclusion that would apply even when it is undisputed that law enforcement has the legal authority to acquire such information.

Second, CDT acknowledges that the draft definition of "call-identifying information" originally excluded location information altogether, but that this language was eventually removed from the statutory definition. CDT Comments at 31; see 140 Cong. Rec. S11056 (Aug. 9, 1994) (draft bill) (call-identifying information "does not include any information that may disclose the physical location of the subscriber * * * "). Far from being merely a cosmetic change, as CDT tries to suggest, this revision is devastating to CDT's position. If Congress had intended to exclude location information from the scope of call-identifying information altogether, as CDT contends, it would have left the location language in the definition of "call-identifying information" itself. The only reason to remove the language from the definition, and to substitute the limited proviso now found in Section 103(a)(2) was to ensure that location information would not be excluded from the scope of call-identifying information in non-pen register cases. The legislative history thus provides compelling evidence that CDT's reading of the statute is incorrect.

B. Packet switching

CDT also objects to provisions of the interim standard that require carriers transmitting communications using packet switching protocols to deliver the entire packet data stream associated with a given communication, including call content, except where information is not authorized to be acquired. CDT asserts that this aspect of the interim standard violates Section 103(a)(4)(A) of CALEA, which requires carriers to "protect[] * * * the privacy and security of communications and call-identifying information not authorized to be intercepted * * * ."

In our May 20 comments, we explained why the packet switching provisions of the interim standard are consistent with Section 103(a)(4)(A). See DOJ/FBI Comments at 21-22. The only additional point that needs to be made is that, to the extent that carriers may find it technically feasible to strip out call content from the packet data stream and deliver only call-identifying information in cases where the government does not have authority to intercept call content (cf. CDT Comments at 36-38), the government has no objection to the implementation of such solutions. In defending the interim standard, it emphatically is not the government's object to obtain access to call content in cases where its legal authority does not extend that far.

C. Covered Carriers

The assistance capability requirements of Section 103 of CALEA apply to "telecommunications carriers," a term that CALEA specifically defines. See 47 U.S.C. § 1001(8). AT&T devotes a relatively lengthy discussion to the issue of whether providers of Cellular Digital Packet Data ("CDPD") services come within the statutory definition of telecommunications carriers. See AT&T Comments at 17-22. This issue is wholly outside the scope of the April 20 Public Notice

governing the present comments, and we therefore reserve discussion on it for a more appropriate setting.

* * *

This proceeding involves issues of great urgency and importance to the American people. As Congress recognized when it enacted CALEA, the ability of federal, state, and local law enforcement agencies to carry out legally authorized electronic surveillance is critical to the effective detection, prosecution, and prevention of criminal activity. What is at stake here is not mere "one-stop shopping" or "convenience" for law enforcement, as the commenters cavalierly suggest, but rather the public's interests in enforcing criminal laws and preserving personal safety -- interests of the highest possible magnitude. Congress has imposed specific assistance capability obligations on telecommunications carriers to further these interests, and Congress has entrusted the Commission with the responsibility to ensure that carriers fully satisfy those obligations. For the reasons given above and in the government's rulemaking petition, prompt action by the Commission is imperative if the assistance capability requirements of CALEA -- and the compelling public interests underlying them -- are to be vindicated.

DATE: June 12, 1998

Respectfully submitted,

Louis J. Freeh, Director
Federal Bureau of Investigation

Honorable Janet Reno
Attorney General of the United States

Larry R. Parkinson
General Counsel
Federal Bureau of Investigation
935 Pennsylvania Avenue, N.W.
Washington, D.C. 20535

Stephen W. Preston
Deputy Assistant Attorney General
Douglas N. Letter
Appellate Litigation Counsel
Civil Division
U.S. Department of Justice
601 D Street, N.W., Room 9106
Washington, D.C. 20530
(202) 514-3602